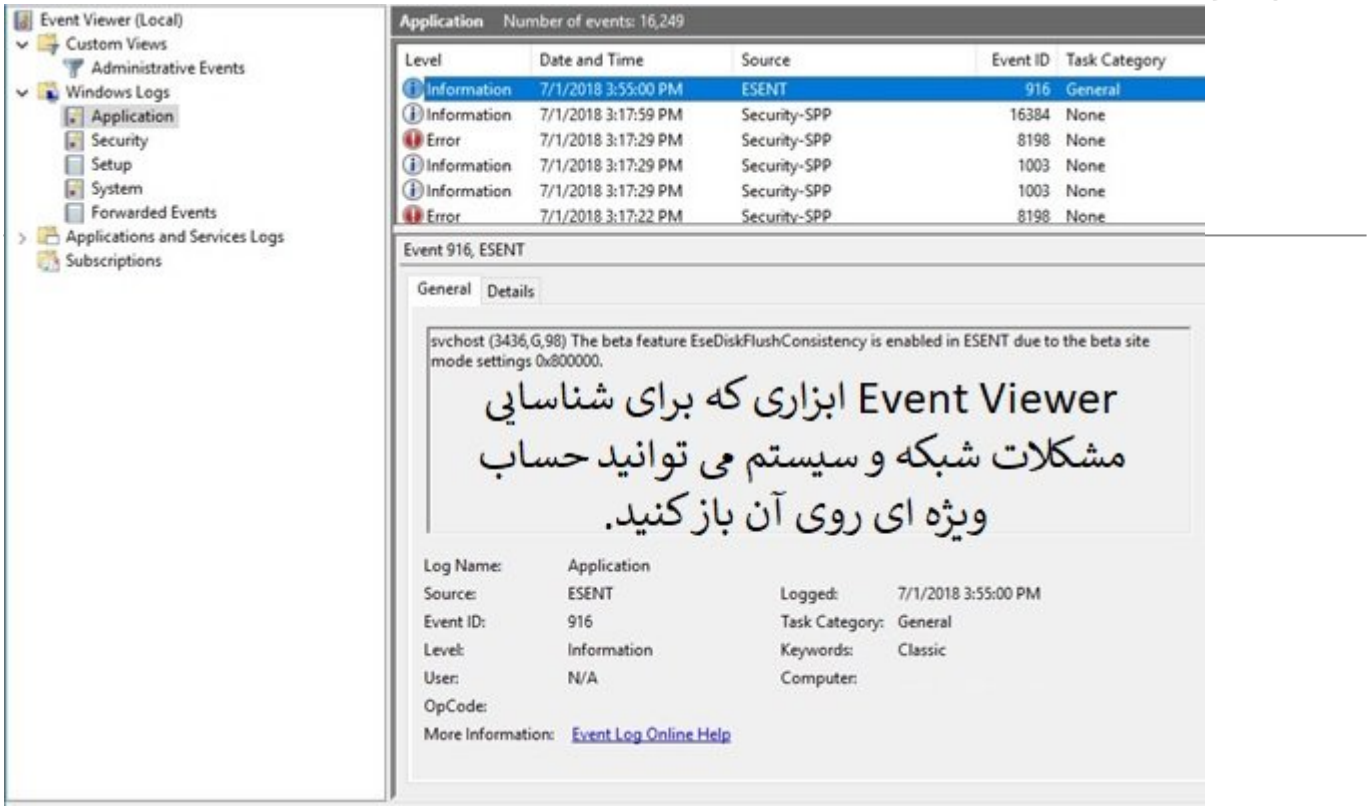
ثبت دقیق رخدادها توسط ناظر رویدادها

راهنمای جامع به‌کارگیری Event Viewer برای شناسایی مشکلات سیستم (بخش اول)



زمانی که به دنبال پیدا کردن مشکلی در یک کامپیوتر متصل به شبکه یا کامپیوتر خانگی هستیم، به سرعت به سراغ اینترنت رفته و در تلاش هستیم تا سنگین‌ترین و جدیدترین نرم‌افزاری که اجازه می‌دهد مشکلات کامپیوتر را شناسایی کرده، پیدا کرده و دانلود کنیم. زمانی که اتصال به یک شبکه بی‌سیم به درستی برقرار نمی‌شود، به سرعت به سراغ تنظیمات روتر می‌رویم، دانگل وای‌فای یا کابل اترنت را بررسی می‌کنیم تا علت بروز مشکل را پیدا کنیم. زمانی که سیستم به واسطه یکسری رفتارهای غیرعادی قادر نیست به فعالیت خود ادامه دهد به سرعت به سراغ گزارش‌های ضدویروسی می‌رویم تا علت بروز مشکل را پیدا کنیم. اما واقعیت این است که بسیاری از کاربران پلتفرم ویندوز از وجود یک مولفه قدرتمند اما در عین حال ناشناخته ویندوز غافل هستند. ویندوز از ماژول‌ها و مولفه‌های مختلفی ساخته شده است که یکی از این مولفه‌ها Event Viewer است.

رویداد چیست؟

رویداد به فعالیتی اشاره دارد که در یک سیستم انجام شده است. یک رخداد می‌تواند از سوی منابع مختلفی تولید شود. این منبع می‌تواند یک برنامه کاربردی یا خود ویندوز باشد. این رخداد که اطلاعات مهمی را ارائه می‌کند درون یک فایل گزارش قرار می‌گیرد. رخدادها به منظور نشان دادن خطاها، اطلاعات، و خرابی‌هایی که در یک سیستم رخ داده تولید می‌شوند. به‌دلیل اینکه رخدادها دارای تنوع زیادی بوده و از منابع مختلفی تولید می‌شوند، ویندوز آن‌ها را دسته‌بندی کرده است. در این دسته‌بندی رخدادها در یکی از زیرگروه‌های رخدادهای سیستمی، رخدادهای امنیتی و رخدادهای برنامه‌ها قرار می‌گیرند. از زمانی که سیستم را راه‌اندازی کرده و به آن وارد می‌شوید ویندوز 10 رخدادهای به وجود آمده در سیستم را ثبت می‌کند. اما توجه به گستردگی بیش از اندازه رخدادها این امکان وجود ندارد تا به شکل آنی و مستمر این گزارش‌ها را به کاربر نشان داد، از این‌رو ویندوز این اطلاعات را جمع‌آوری کرده و در یک مکان مشخص به کاربر نشان می‌دهد. این سرویس که در حقیقت یکی از مولفه‌های ویندوز است Event Viewer نام دارد. وظیفه Event Viewer ثبت رخدادها به‌صورت تفکیک شده در فایل‌های مختلف است.

Application Log

اطلاعات قرار گرفته در این بخش به رویدادهای تولید شده از برنامه‌ها اشاره دارند. این رویدادها می‌توانند اطلاعاتی در ارتباط با یک برنامه و مشکلاتی که برای یک برنامه به وجود آمده است را شامل شوند. کارشناسان حرفه‌ای از این بخش برای شناسایی مشکلات برنامه‌ها استفاده می‌کنند.

Security Log

رویدادهایی امنیتی مواردی مانند تلاش‌های ناموفق ورود به سیستم، رویدادهای مرتبط با منابع سیستمی، عملیاتی که

روی فایل‌ها اجرا شده یا تغییراتی که روی فایل‌های سیستمی به وجود آمده است را شامل می‌شوند.

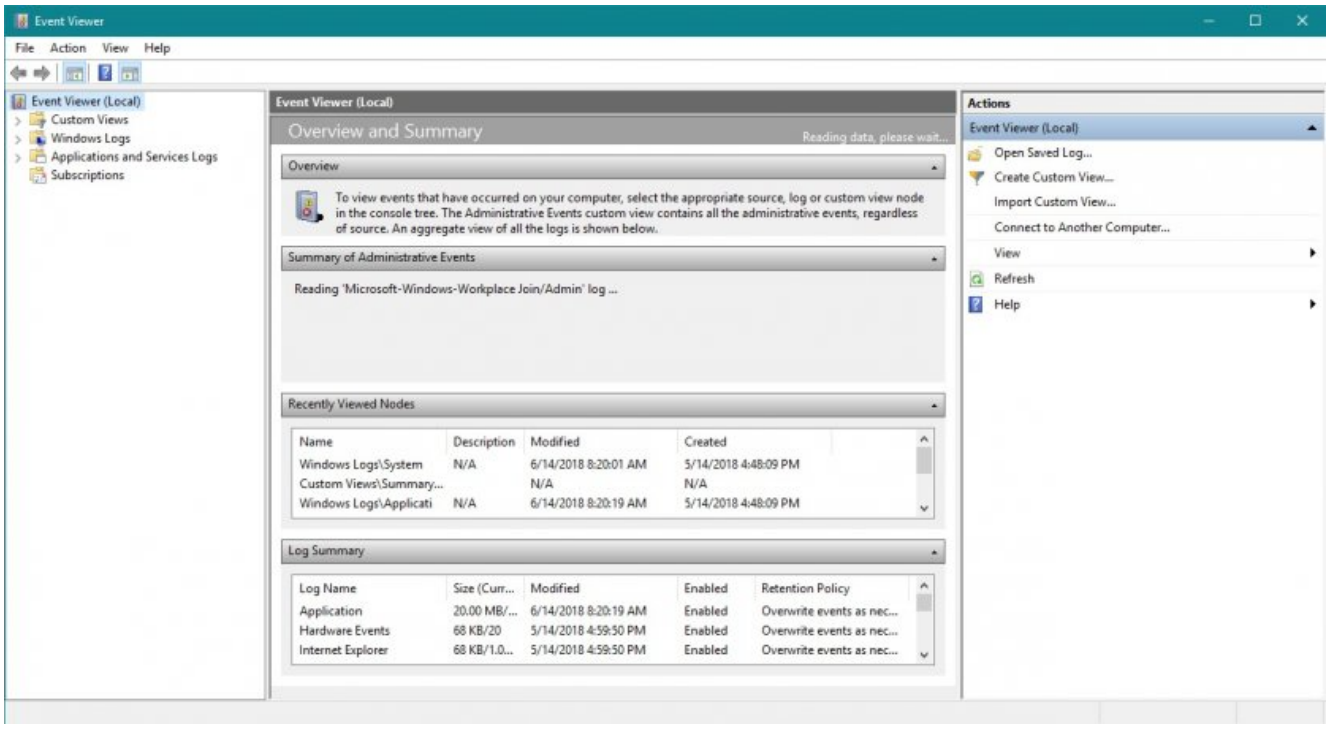
System Log

رویدادهای قرار گرفته در این بخش در ارتباط با مولفه‌های سیستم‌عامل ، خرابی یک درایور در زمان بارگذاری و مواردی از این دست هستند.

سه گروهی که به آنها اشاره گردید در برنامه Event Viewerدر زیر شاخه Windows Logs که در ادامه با آن‌ها آشنا خواهید شد قرار دارند.

اجرای برنامه

در ویندوز 10 در کادر جست‌وجو عبارت Event Viewer را تایپ کرده و روی گزینه پیدا شده کلیک کنید. Event Viewer از قسمتهای مختلفی تشکیل شده است. پانل سمت چپ در برگیرنده گزینه‌هایی است که هر کدام رویدادهای مختلف را به‌صورت طبقه‌بندی شده در خود جای داده‌اند. در پانل سمت راست یکسری فرامین و وظایف قرار دارند که با استفاده از آن‌ها می‌توانید روی رویدادها کنترل داشته و آن‌ها را سازمان‌دهی کنید. اصلی‌ترین بخش که شامل پنجره‌های مختلفی برای نمایش اطلاعات است در وسط برنامه قرار دارد. اولین قسمت این بخش Overview نام دارد که در برگیرنده توضیحاتی در ارتباط با برنامه فوق است.



Summary of Administrator Events

در این بخش خلاصه‌ای از رویدادهای در سطح مدیریتی سیستم را مشاهده می‌کنید.همان‌گونه که در شکل زیر مشاهده می‌کنید هر بخش شامل اطلاعاتی است که به صورت تفکیک شده برای نشان دادن زمان‌های بحرانی، خطاها، هشدارها، عملیاتی که اجرای آن‌ها با موفقیت همراه بوده مورد استفاده قرار می‌گیرد.

Summary of Administrative Events

Event Type	Event ID	Source	Log	Last hour	24 hours	7 days
Critical	-	-	-	0	0	0
⊞ Error	-	-	-	1	17	41
⊞ Warning	-	-	-	0	6	342
⊞ Information	-	-	-	44	426	1,942
⊞ Audit Success	-	-	-	210	411	809

همچنین، برای هر بخش ستون‌هایی وجود دارد که با استفاده از این ستون‌ها می‌توانید تعداد خطاهایی که در یک ساعت، یک روز یا یک هفته گذشته رخ داده‌اند را مشاهده کنید. اگر روی هرکدام از این گزینه‌ها کلیک کنید جزئیات مربوط به هر گزینه قابل مشاهده است.

Recently Viewed Nodes

آخرین رخدادهای به وقوه پیوسته در سیستم در این بخش قابل مشاهده است.

Log Summery

خلاصه‌ای از رخدادهای ثبت شده در سیستم در این پانل نشان داده می‌شود. اگر روی یک رخداد کلیک راست کرده و گزینه View Events in this log را انتخاب کنید، به‌طور مستقیم به بخشی که رخداد به آن تعلق دارد هدایت خواهید شد. رخدادهایی که در این بخش نشان داده می‌شوند در فایل‌هایی مجزا قرار دارند که هر فایل بیانگر یک گروه ویژه از رخدادها است.

مشاهده رویدادها

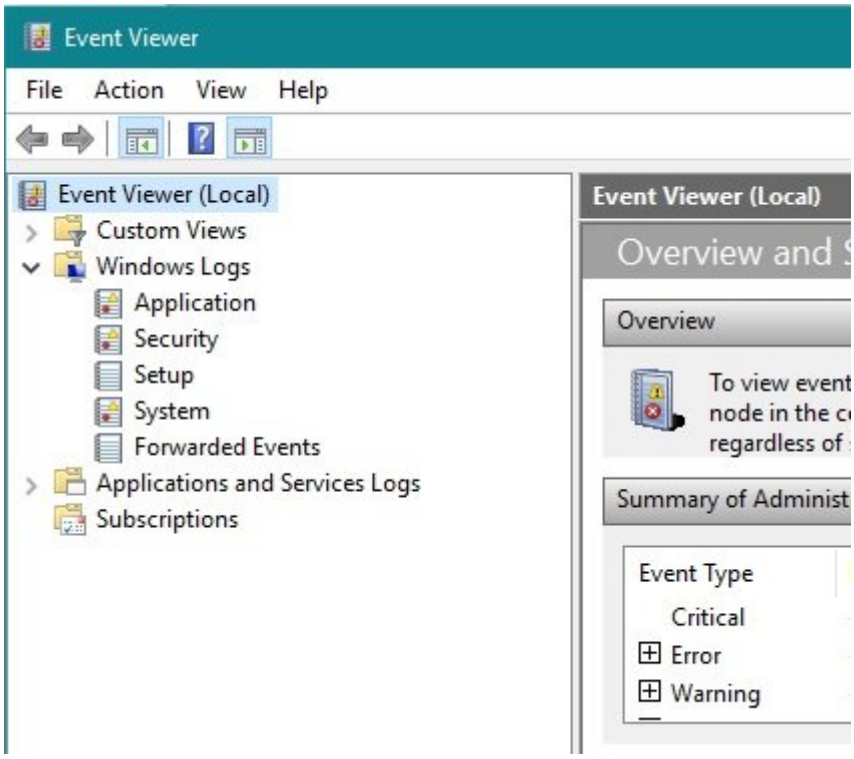
سمت چپ Event Viewer دسترسی به رویدادهای مختلف را بر مبنای نوع آن‌ها مکان‌پذیر می‌کند. همان‌گونه که در شکل زیر مشاهده می‌کنید در زیر شاخه Event Viewer(Local) یکسری پوشه اصلی قرار دارد که هر کدام دربرگیرنده گزینه‌های مختلفی هستند.

Log Summary

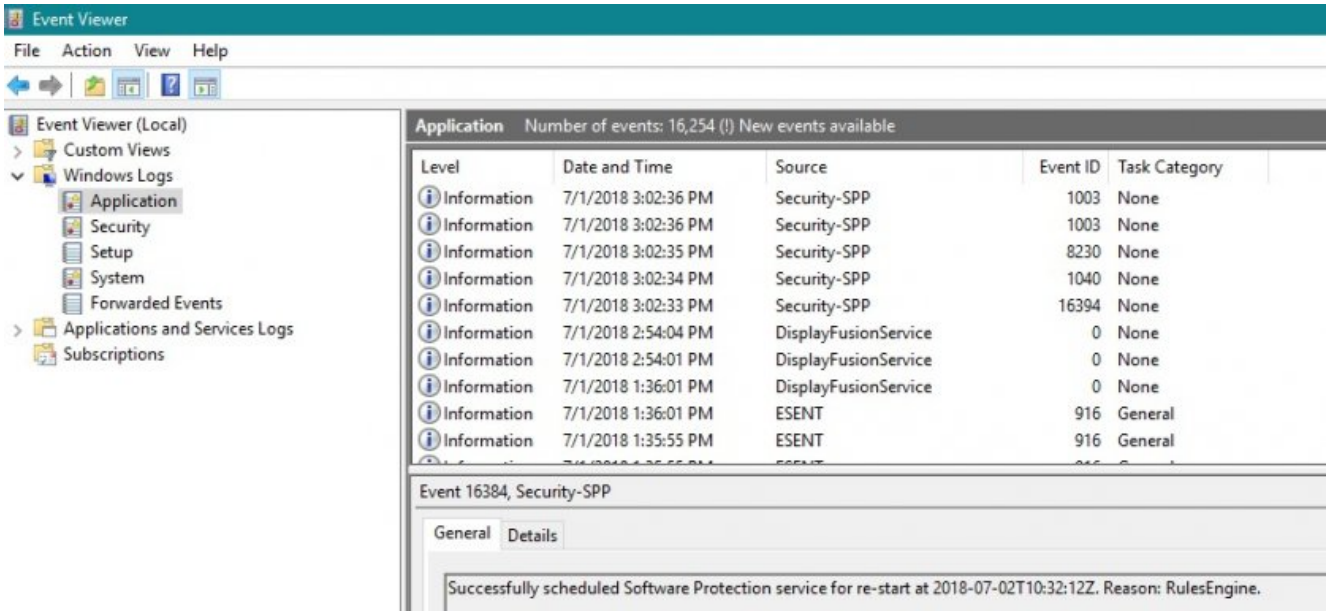
Log Name	Size (Current/Ma...	Modi...	Enabled	Retention Policy
Application	1.07 MB/20 MB	1/25/...	Enabled	Overwrite events as necessary ...
Hardware Events	68 KB/20 MB	1/22/...	Enabled	Overwrite events as necessary ...
Internet Explorer	68 KB/1.00 MB	1/22/...	Enabled	Overwrite events as necessary ...
Key Management Service	68 KB/20 MB	1/22/...	Enabled	Overwrite events as necessary ...

به‌طور مثال اگر روی گزینه Windows Logs کلیک کنید سه گزینه اصلی Application/Security/System که درون آن قرار دارد را مشاهده می‌کنید که با کلیک روی هر کدام رویدادهای بخش مربوطه به آن گزینه همراه با جزییات نشان داده می‌شود. اگر پوشه Windows Logs را باز کنید، گزینه‌هایی که در شکل بالا مشاهده می‌کنید در اختیارتان قرار می‌گیرد. هر کدام از گزینه‌های این بخش بیان‌گر رخداد خاصی هستند که در ابتدای مقاله به آن‌ها اشاره کردیم. فایل‌هایی که گزارش‌های مربوط به رخدادها را نگه می‌دارند با فرمت فایلی evxt قابل تشخیص هستند. به‌طور مثال اگر روی گزینه Application کلیک کنید، رویدادهایی که توسط برنامه‌های مختلف تولید شده‌اند را مشاهده خواهید کرد. اطلاعات قرار گرفته در شاخه Application در مسیر
%SystemRoot%\System32\Winevt\Logs\Application.evtx قرار دارند.

همانگونه که در شکل زیر مشاهده می‌کنید، رویدادهای مربوط به برنامه‌ها به همراه اطلاعات بیشتری در ستون‌هایی به کاربر نشان داده می‌شوند.



اطلاعات ارائه شده در این ستون‌ها در قالب خطا، هشدار یا پیغام وضعیت یک برنامه را تشریح می‌کنند. به‌طور مثال اگر برنامه‌ای به دلیل بروز یک خطا به‌طور ناگهانی خاتمه پیدا کرده و برنامه موفق نشده باشد خطای به وجود آمده را طرف کند پیغام خطایی در این بخش ثبت خواهد شد. گزینه Custom Views یکی از گزینه‌های مهم قرار گرفته در زیر شاخه Event Viewer است که برای مشاهده دلخواه رویدادها، خطاها و هشدارها به کار گرفته می‌شود. زمانی‌که روی این گزینه کلیک می‌کنید، جزییات مربوطه همانند شکل زیر نشان داده می‌شود.



اطلاعات ارائه شده از سوی این گزینه به دو گروه تقسیم شده و به کاربر نشان داده می‌شود. در بالای پنجره رویدادها به‌همراه تاریخ، زمان و منبعی که آن‌ها را تولید کرده‌اند قابل مشاهده هستند. زمانی‌که روی هر رویداد کلیک کنید در قسمت پایین پنجره توضیحات مربوط به آن رویداد قابل مشاهده است. این قسمت از دو زبانه General/Details تشکیل شده است. در زبانه General توضیحی در مورد رخداد انتخاب شده ارائه می‌شود. در این پنجره می‌توانید علت و نوع رخداد را با اطلاعات بیشتری مشاهده کنید. همچنین یکسری توضیحات برای درک بهتر خطای رخ داده ارائه می‌شوند که این توضیحات مواردی همچون نام، نوع و مبدا رخداد ثبت شده، زمان ثبت رخداد، شناسه رخداد، سطح رخداد، کاربری که در زمان اجرای رخداد در سیستم فعال بوده، کلمه یا کلمات کلیدی

رخداد و کامپیوتری که رخداد در آن بوجود آمده و در نهایت دسترسی آنلاین برای دریافت جزییات بیشتر را شامل می‌شود. زبانه Detail جزییاتی که به آن‌ها اشاره شد را با نکات بیشتری ارائه می‌کند. در این زبانه می‌توانید اطلاعات را در قالب Friendly View یا Xml View مشاهده کنید. به‌طور مثال، در این زبانه می‌توانید شناسه مربوط به پردازه‌ها و ریسمان‌ها را مشاهده کنید. اگر روی گزینه xml کلیک کنید این اطلاعات در قالب فرمت xml نشان داده می‌شود.

تاریخ انتشار:

22 آبان 1397

نشانی منبع:
https://www.shabakeh-mag.com/workshop/13830/%D8%B1%D8%A7%D9%87%D9%86%D9%85%D8%A7%DB%8C-%D8%AC%D8%A7%D9%85%D8%B9-%D8%A8%D9%87%E2%80%8C%DA%A9%D8%A7%D8%B1%DA%AF%DB%8C%D8%B1%DB%8C-event-viewer-%D8%A8%D8%B1%D8%A7%DB%8C-%D8%B4%D9%86%D8%A7%D8%B3%D8%A7%DB%8C%DB%8C-%D9%85%D8%B4%DA%A9%D9%84%D8%A7%D8%AA-%D8%B3%DB%8C%D8%B3%D8%AA%D9%85-%D8%A8%D8%AE%D8%B4-%D8%A7%D9%88%D9%84