رفع‌اشکال ویندوز۷ با فایل‌های Log و برنامهٔ Event Viewer

برای آدم‌های منظم و مرتب روی می‌دهد. در ترافیک سنگین به محل کار خود می‌روید، یک چای می‌نوشید، و به طرف کامپیوتر می‌روید تا روز کاری خود را آغاز کنید. به جای دیدن **کاغذ دیواری** انتخابی خودتان بر روی صفحه‌نمایش ـ همان تصویری که ممکن است شما را به یاد زندگی در خارج از محیط کار بیندازد ـ یک پنجرهٔ کوچک به نمایش درمی‌آید و به شما اطلاع می‌دهد که **ویندوز** با نوعی خطا مواجه شده است. حتی اگر این پیام خطا شرحی از مسئله داده باشد، بازهم در فهمیدن این که اشکال دقیقاً در کجاست سردرگم می‌شوید.

ویندوز۷ هر چیزی را که در زمان بیداری روزانهٔ خودش رخ می‌دهد ثبت می‌کند، و شما می‌توانید این اطلاعات را برای رفع‌اشکال مسائل سیستم به کار بگیرید. **فایل‌های واقعه‌نگار** (log file) که **ویندوز۷** می‌سازد می‌توانند برای حل مسائل بسیار سودمند باشند، و مایکروسافت کاری کرده است که به‌دست‌آوردن، فهمیدن، و به‌کارگیری این داده‌ها برای حل مسائل آسان شود. یک **فایل واقعه‌نگار** مانند همان جعبه‌سیاه کوچک بر روی یک هواپیماست، که فعالیت‌های **ویندوز۷** را در زمانی که کامپیوتر در حال کار است ثبت می‌کند. یادگیری نحوهٔ دستیابی و فهمیدن اطلاعات فهرست‌شده در **فایل‌های واقعه‌نگار** به شما کمک خواهد کرد که یک نگاه واضح‌تر به عملیات اجراشده داشته باشید تا بهتر بتوانید مسائل را حل کنید، و زمان تشخیص عیب را کوتاه کنید.

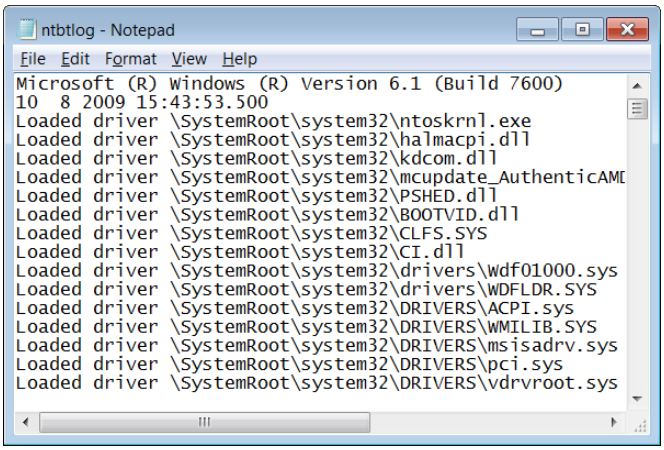
مسائل بوت

اگر در زمانی که ویندوز شروع به کار می‌کند مسئله‌ای رخ بدهد، احتمال این که **برنامه‌های رانش‌گر** (device driver) مشکل داشته باشند زیاد است. **برنامهٔ رانش‌گر** یک فایل یا مجموعه‌ای از فایل‌هاست که به **سیستم‌عامل** می‌گوید که چگونه با یک وسیله یا دستگاه خاص ارتباط برقرار کند. در زمان راه‌اندازی، **ویندوز** برای هر وسیله، از دیسک‌ران سی‌دی‌نویس گرفته تا صفحه‌کلید، یک رانش‌گر را بار می‌کند. مسائلی که در زمان راه‌اندازی رخ می‌دهند می‌توانند دردسرآفرین، و پیداکردن علت آنها دشوار باشد. با فعال‌کردن **boot logging** (واقعه‌نگاری به هنگام عملیات بوت)، **ویندوز** یک **فایل واقعه‌نگار** متنی برای ثبت رانش‌گرهایی که در زمان راه‌اندازی بار می‌شوند و این که بارشدن آنها موفقیت‌آمیز یا ناموفق بوده است می‌سازد. **ویندوز۷** به طور خودکار این اطلاعات را به هنگامی که به حالت Safe Mode بوت کنید ذخیره می‌کند، اما شما معمولاً به بوت عادی به **ویندوز۷** نیاز خواهید داشت، چون حالت Safe Mode فقط رانش‌گرهای ضروری برای راه‌اندازی ویندوز را بار می‌کند. واقعه‌نگاری به هنگام عملیات بوت (boot logging) را در زمان راه‌اندازی به محض دیدن اولین صفحهٔ راه‌اندازی **ویندوز۷** با زدن کلید F8 می‌توانید فعال کنید. منوی زیر ظاهر خواهد شد:

Advanced Boot Options

که چند گزینهٔ مفید بوت را فراهم می‌سازد. گزینهٔ Enable Boot Logging را انتخاب کنید.

ویندوز۷ به بوت‌کردن طبیعی خود ادامه خواهد داد، و رانش‌گرها را برای همهٔ وسایل پیشتر نصب‌شده بار خواهد کرد. **ویندوز** حالا نتایج هر تلاش خود برای بارکردن یک رانش‌گر را در یک فایل متنی با دسترسی‌پذیری آسان ثبت خواهد کرد. این فایل، **Ntbtlog.txt**، در دیرکتوری C:\Windows قرار دارد. **ویندوز** این اطلاعات را به یک log یا فایل واقعه‌نگاری پیشترثبت‌شده اضافه می‌کند، در نتیجه، آخرین اطلاعات را در انتهای فایل خواهید دید. فایل Ntbtlog.txt را در برنامهٔ Notepad باز کنید و خطاهای آن را بررسی کنید.



اگر کامپیوتر در زمان راه‌اندازی قفل کند، مجبورید کامپیوتر را در حالت Safe Mode راه‌اندازی کنید تا این فایل را ببینید، و یا مجبورید کامپیوتر را با دیسک نصب **ویندوز۷** خود بوت کنید، و از System Recovery Options برای دیدن این فایل بهره بگیرید.

در System Recovery Options گزینه Command Prompt را انتخاب کنید، و در نشانه فرمان **notepad** را تایپ کنید و کلید Enter را بزنید. حال، فایل Ntbtlog.txt را در برنامهٔ Notepad باز کنید.

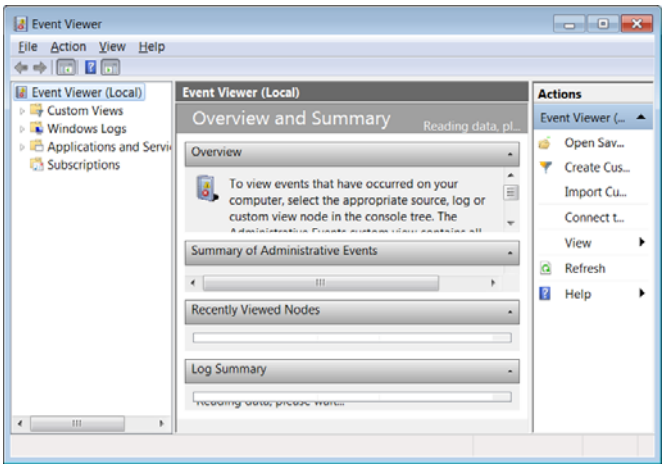
اگر **فایل واقعه‌نگار** مشخص کند که یک فایل ویژه مربوط به یک رانش‌گر بار نشده است، علت می‌تواند یکی از موارد زیر باشد: آن فایل حذف شده است، خراب شده است، وابسته به رانش‌گر دیگری است که به طور موفق بار نشده است، یا طوری میزان شده است که طبق درخواست یک رانش‌گر دیگر به طور دستی بار شود. همچنین ممکن است که دستگاه مربوط به آن فایل رانش‌گر در بخش Device Manager **ویندوز** غیرفعال شده باشد. ممکن است لازم باشد که رانش‌گرها را از نو نصب، روزآمد یا فعال کنید تا مسئله حل شود.

با آن که Boot Logging یک روش عالی برای بررسی مسائل راه‌اندازی **ویندوز** است، محدودیت‌هایی نیز دارد. اگر خطا در زمان عملیات راه‌اندازی خیلی زود یا خیلی دیر رخ بدهد، یا ربطی به یک رانش‌گر نداشته باشد، فایل واقعه‌نگار بوت در ردیابی علت مسئله به شما کمک نخواهد کرد. **ویندوز** یک برنامهٔ قدرتمندتر به نام **Event Viewer** دارد که پیوسته اطلاعات مهمی را ثبت می‌کند که ممکن است در ردیابی علت مسئله به شما کمک کنند.

برنامهٔ Event Viewer

برنامهٔ Event Viewer یک برنامهٔ عالی برای استفاده در زمان رفع‌اشکال کامپیوتر است، و بهتر از همه، رایگان است و در خود **ویندوز** گنجانده شده است. برنامهٔ Event Viewer را می‌توانید از طریق نماد Administrative Tools در System and Security در Control Panel، یا تایپ **Event Viewer** در کادر جستجوی منوی Start پیدا کنید.

در ستون سمت چپ پنجرهٔ اصلی چهار پوشهٔ Custom Views، Windows Logs، Applications and Services Logs، و Subscriptions به نمایش درمی‌آید.



پوشهٔ Windows Logs

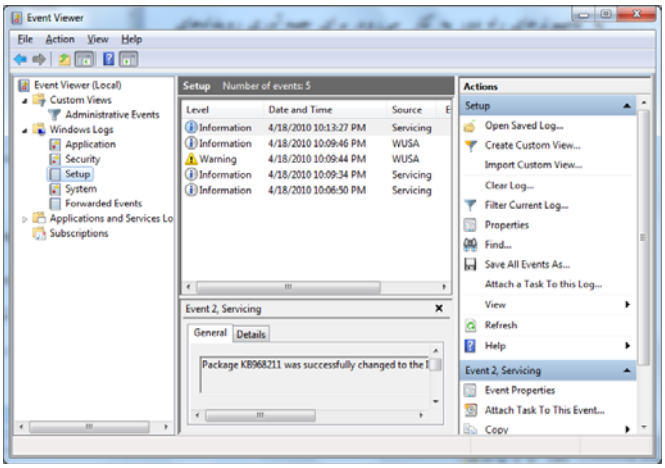
پوشهٔ Windows Logs را باز کنید. رویدادهای (events) این پوشه به پنج گروه تقسیم شده‌اند: Application، Security، Setup، System، و Forwarded Events.

● **Application**. این گروه حاوی رویدادهایی است که در برنامه‌های کاربردی شما رخ می‌دهند. به عنوان مثال، یک رویداد برنامهٔ کاربردی می‌تواند یک تغییر در پیکربندی، یک فایل گمشده، یا یک ارتباط راه‌دور قطع‌شده را ثبت کند.

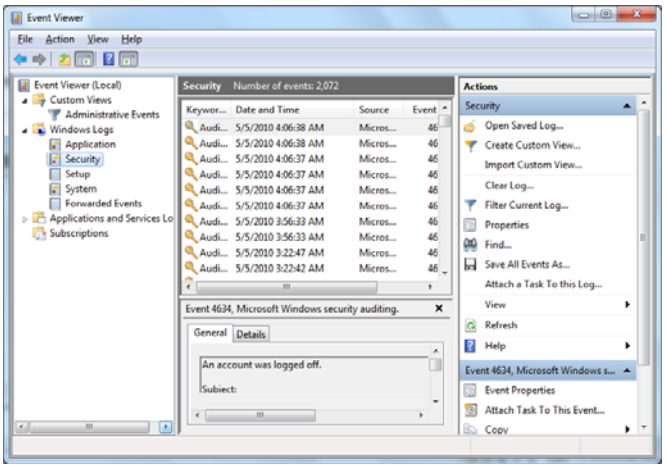
● **System**. واقعه‌نگار سیستم همهٔ رویدادهایی را نشان می‌دهد که به **ویندوز** مربوط هستند. دفترچهٔ خاطرات مجازی **ویندوز** است که همهٔ عملیات را برای هر بخش سیستمی، شامل **سرویس‌های** زمینه‌ای، دستگاه‌ها، و بخش‌های شبکه ردیابی می‌کند. به عنوان مثال، عیب در یک رانش‌گر یا یک برنامه سیستمی دیگر که لازم است در زمان راه‌اندازی **ویندوز** بار شوند در این بخش ثبت می‌شود.

● **ForwardedEvents**. برای ذخیره رویدادهای مربوط به کامپیوترهای راه دور به کار می‌رود. برای جمع‌آوری رویدادهای کامپیوترهای راه دور، باید یک **اشتراک رویداد** (event subscriptions) بسازید که از عهده این مقاله خارج است.

● **Setup**. حاوی رویدادهای مربوط به برپایی برنامه‌های کاربردی است.

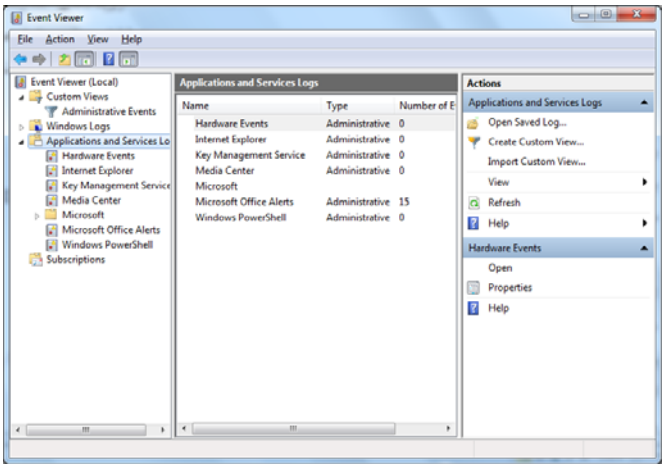


● **Security**. بخش Security حاوی رویدادهایی مانند تلاش‌های ورود به حساب کاربری معتبر و نامعتبر، و همچنین رویدادهای مربوط به مصرف منابع، مانند ساخت، بازکردن، یا حذف فایل است. مدیران می‌توانند مشخص کنند که کدام وقایع در بخش Security ثبت شوند. **گروه امنیتی** (Security) همهٔ رویدادهایی را ثبت می‌کند که به سیاست‌های امنیتی مربوط است. رویدادهای امنیتی، مانند دستیابی فایل و ساخت فایل، logonهای کاربری، و تغییرات سیاست، در اینجا به نمایش در خواهند آمد. به طور پیش‌گزیده (default)، واقعه‌نگاری امنیتی در **ویندوز۷** فعال نمی‌شود. یک مدیر (administrator) باید یک بستهٔ واقعه‌نگاری امنیتی را در سیستم‌عامل نصب و مشخص کند که کدام نوع رویدادهای امنیتی تحت نظر قرار بگیرند. پیکربندی این نوع واقعه‌نگاری خارج از عهدهٔ این مقاله است، در نتیجه، عمدتاً روی دستیابی و به‌کارگیری خود فایل‌های واقعه‌نگار توجه خواهیم کرد.



پوشه Applications and Services Logs

بخش Applications and Services Logs یک گروه جدید از رویدادهایی است که ثبت می‌شود. این بخش رویدادهای مربوط به برنامه‌های کاربردی‌ای را که ممکن است اثر سیستمی نداشته باشند ثبت می‌کند.



این گروه حاوی چهارگونه رویداد است: Admin، Operational، Analytic، و Debug. رویدادهای واقع در بخش Admin به ویژه مورد علاقه متخصصان IT است که با Event Viewer رفع اشکال می‌کنند. بخش Debug بیشتر مورد استفاده سازندگان برنامه‌های کاربردی

است. هر دو بخش Analytic و Debug به طور پیش‌فرض غیرفعال و پنهان هستند. برای نمایش آنها در منوی View گزینه Show Analytic and Debug Logs را انتخاب کنید.

•رویدادهای Admin

رویدادهایی که در بخش Admin ثبت می‌شوند یک مسئله و یک راه حل آن را مشخص می‌کنند. یک مثال از یک رویداد Admin رویدادی است که به هنگامی که یک برنامه کاربردی در برقراری ارتباط با یک چاپگر ناتوان باشد رخ می‌دهد. این رویدادها دستورالعمل‌های حل مسئله را فراهم می‌کنند.

•رویدادهای Operational

رویدادهای Operational برای تجزیه و تحلیل و تشخیص یک مسئله یا رویداد به کار برده می‌شوند. یک مثال از رویدادهای Operational وصل‌شدن یا جداشدن یک چاپگر است.

•رویدادهای Analytic

رویدادهای Analytic در حجم زیاد انتشار می‌یابند و عملیات برنامه را توصیف می‌کنند و مسائلی را مشخص می‌کنند که بدون دخالت کاربر ممکن است روی بدهند.

•رویدادهای Debug

رویدادهای Debug مورد استفاده برنامه‌سازان برای رفع اشکال برنامه است.

مشخصه‌های رویدادها و رفع‌اشکال بر اساس این مشخصه‌ها

در زیر بعضی از مشخصه‌های عمومی هر رویداد معرفی شده است: **Level**، **Source**، و **EventID**.

Level موقع رفع‌اشکال، مهم است که **سطح** یا **Level** رویدادهای هر گروه را ببینید. **Level** نوعی طبقه‌بندی شدت اثر رویداد است. سطوح شدتی زیر در رویدادهای سیستمی و برنامه‌های کاربردی ممکن است رخ بدهد: Information، Warning، Error، Critical، Success Audit، و Failure Audit.

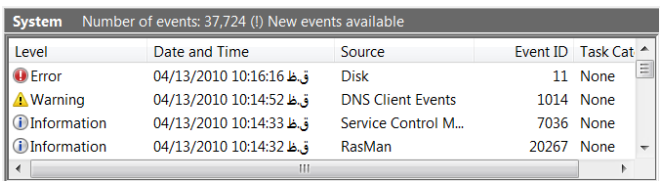
- **رویدادهای اطلاعاتی** (Information events) عملیاتی را ثبت می‌کنند که به طور موفق به اجرا درمی‌آیند، مانند سرویس‌هایی که راه‌اندازی می‌شوند یا وسایلی که سیستم آنها را متوقف کرده است.

رویداد اطلاعاتی مشخص می‌کند که در یک برنامه کاربردی یا یک بخش از یک برنامه بزرگ یک تغییر رخ داده است، مانند تکمیل موفقیت‌آمیز یک برنامه کاربردی، یا شروع به کار یک سرویس.

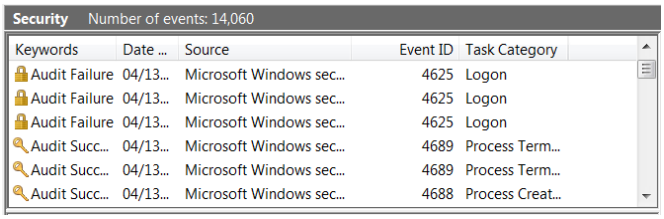
•**رویدادهای هشداردهنده** (Warning events)، که با یک نماد زرد علامت‌گذاری می‌شوند، مشخص می‌کنند که **ویندوز** در اجرای یک تکلیف سردرگمی‌هایی داشته است، اما خودش می‌توانسته است با مسئله کنار بیاید. این نوع رویدادها علائم موشکافانه‌ای هستند که نشان می‌دهند یک جای کار ایراد دارد و می‌تواند به مسئله بینجامد.

•**رویدادهای خطا** (Error events) نشان می‌دهند که یک خطای اساسی رخ داده است و **ویندوز** نمی‌تواند مسئله را تصحیح کند. این خطاها، که با نماد ترس‌آور قرمز علامت‌گذاری می‌شوند، نشان می‌دهند که چیزی درست کار نمی‌کند و این که مسئله در حال حاضر روی کامپیوتر شما اثرگذار است.

•**رویداد بحرانی** (**Critical**) مشخص می‌کند که عیبی رخ داده است که برنامه یا جزء برنامه‌ای که رویداد را به وجود آورده است نمی‌تواند به طور خودکار برطرف شود.



● **ردگیری موفق** (Success Audit) به دستیابی امنیتی موفق اشاره دارد، مانند ورود به سیستم، در حالی که **ردگیری ناموفق** (Failure Audit) به رویدادهایی مانند عدم موفقیت در دستیابی یک دیسک‌ران دلالت دارد.



Source. نرم‌افزاری که رویداد را ثبت کرده است، که می‌تواند نام یک برنامه، مانند SQL Server یا بخشی از سیستم یا یک برنامه بزرگ باشد، مانند نام یک رانش‌گر.

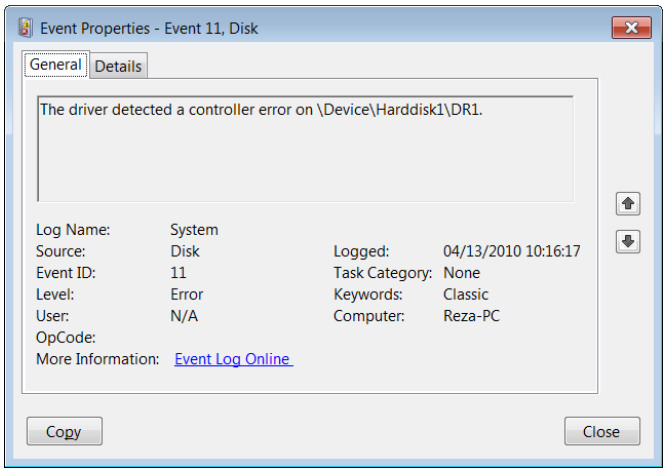
Event ID. شماره معرفی‌کننده نوع یک رویداد.

عیب‌یابی

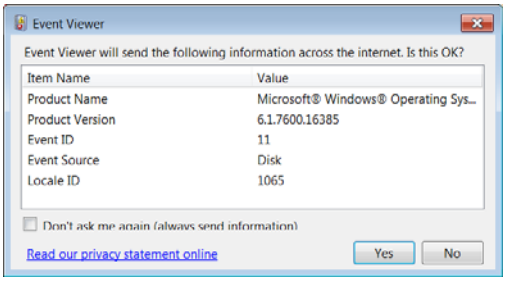
برای پیداکردن رویدادهایی که در حل مسئلهٔ کامپیوترتان کمک خواهند کرد آنها را براساس زمانی که یک خطای مشکوک رخ داده است، نوع رویدادی که رخ داده است، یا منبعی که رویداد را ثبت کرده است مرتب کنید. همچنین رویدادها را می‌توانید طبق گروه، شمارهٔ رویداد، یا نام‌های کامپیوترها و کاربرانی که تحت تأثیر بوده‌اند مرتب (sort) کنید. برای مرتب‌کردن رویدادها، روی عنوان ستون میدانی که می‌خواهید مرتب کنید کلیک کنید.

اگر logها حاوی مقادیر زیادی از داده‌ها باشند، منوی View به شما امکان خواهد داد که نحوهٔ جستجو را برای پیداکردن یک رویداد مشخص کنید. همچنین می‌توانید فهرست رویدادها را برای نمایش صرف رویدادهایی که با خصوصیات ویژه‌ای همسانی دارند، مانند نوع یا منبع رویداد، فیلتر کنید. ما دریافته‌ایم که فیلترکردن رویدادها براساس زمان و تاریخ بسیار سودمند است، زیرا یک خط زمانی دیجیتالی از فعالیت‌های سیستم به هنگام یک دورهٔ زمانی مشخص‌شده را فراهم می‌سازد.

هرگاه یک رویداد مشکوک را یافتید، روی آن رویداد کلیک-دوضرب کنید تا پنجرهٔ Event Properties باز شود. همهٔ اطلاعات دربارهٔ این رویداد به نمایش درخواهد آمد، و برگهٔ Details اطلاعات بیشتری دربارهٔ این رویداد نشان خواهد داد.



اگر این رویداد منطبق با مسئلهٔ خاص شما باشد، روی لینک Event Log Online کلیک کنید.این کار شما را برای اطلاعات بیشتر دربارهٔ این خطا به اینترنت وصل خواهد کرد و شامل مراحلی برای کمک به شما در حل مسئله خواهد بود. با آن که Help And Support Center اطلاعاتی را فراهم می‌کند که مایکروسافت دربارهٔ یک خطا گردآوری کرده است، با استفاده از پایگاه جستجوگر محبوب خود می‌توانید یک پاسخ عمومی به دست بیاورید.



متن پیام خطا را در یک پایگاه جستجوگر تایپ کنید تا یک راه‌حل براساس تجربهٔ کسی دیگر که مسئلهٔ شما را داشته است پیدا کنید. احتمال این که شما اولین شخصی نباشید که با چنین خطایی برخورد کرده‌اید و این که کسی دیگر این مسئله را حل کرده باشد و راه‌حل‌های خود را در جایی در اینترنت ثبت کرده باشد زیاد است. **خبرگروه‌ها** (newsgroup) و انجمن‌های پشتیبانی در اینترنت مکان‌های بسیار خوبی برای این نوع اطلاعات هستند، و درخواست کمک، به‌یقین، صندوق پستی شما را با نظرات و پیشنهادات مختلف برای حل مسئله پرخواهد کرد.

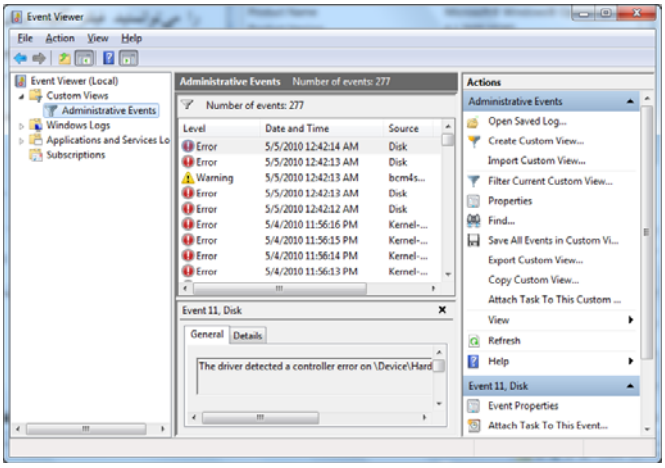
به مرور زمان، واقعه‌نگارهای Event Viewer می‌توانند بسیار بزرگ شوند، در نتیجه، یک فکر خوب آن است که هر چند وقت یک بار فایل‌های واقعه‌نگار را پاک کنید. منوی Action به شما امکان

خواهد داد که فایل‌های واقعه‌نگار را ذخیره، باز، صادر، و پاک کنید. اگر در کامپیوتر خود زیاد با مسئله برخورد می‌کنید، یا دوست دارید که از واقعه‌نگار خود آرشیو تهیه کنید، آنها را پیش از پاک‌کردن در یک فایل ذخیره کنید. به هنگام ذخیرهٔ یک فایل واقعه‌نگار، تاریخ روز را در نام فایل بگنجانید تا بعدها در صورت نیاز به آسانی بتوانید آن را بازیابی کنید. فایل‌های واقعه‌نگار ذخیره‌شده را فقط با بازکردن در برنامهٔ Event Viewer می‌توان به نمایش در آورد، اما یک فایل واقعه‌نگار را در یک فایل متنی نیز می‌توانید ذخیره کنید تا بتوانید در برنامه‌های واژه‌پرداز مانند Notepad نیز آنها را تماشا کنید. ذخیرهٔ فایل واقعه‌نگار به صورت متنی، نه‌تنها به شما امکان خواهد داد که واقعه‌های خطا را ایمیل یا چاپ کنید، بلکه به شما اجازه خواهد داد که داده‌ها را برای انتقال از طریق اینترنت، cut و paste کنید.

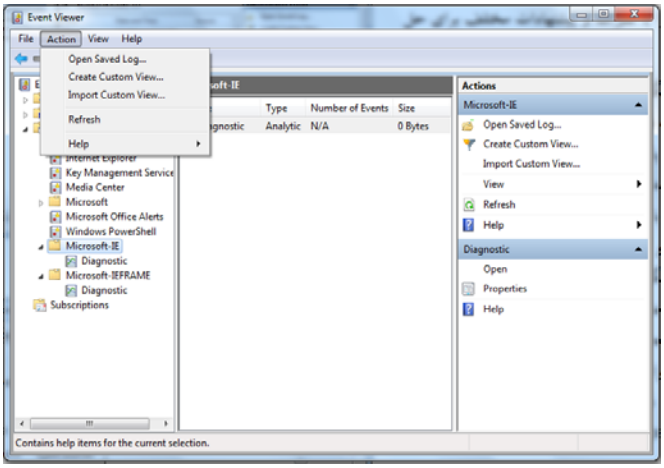
نمایش اختصاصی (Custom Views)

در نگارش های پیشین Event Viewer، رویدادهای یک فهرست را می‌توانستید فیلتر کنید. برای فیلترکردن، مجموعه‌ای از قواعد را مشخص می‌کردید که برای تعیین این که کدام رویدادها در فهرست بیایند و کدام‌ها پنهان شوند به کار می‌رفتند. به عنوان مثال می‌توانستید مشخص کنید که فقط رویدادهای با سطح Error یا Warning به نمایش دربیایند.

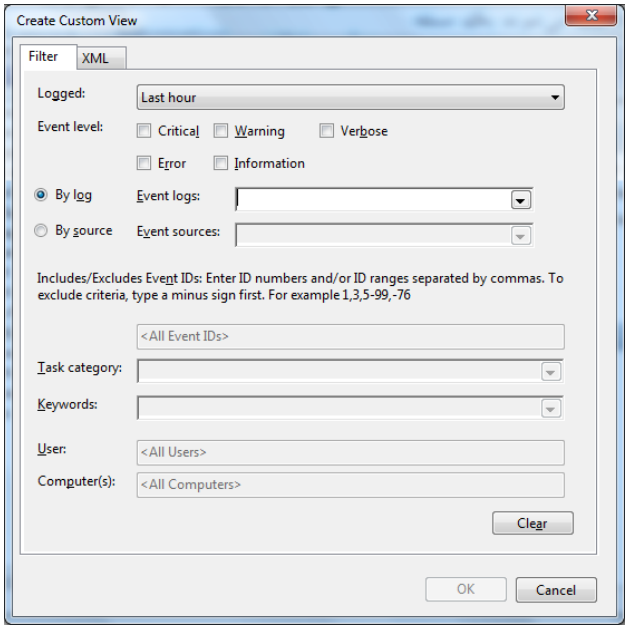
برنامه جدید Event Viewer این امکان را برای شما فراهم می‌آورد که رویدادهای مربوط به منابعی که شما مشخص می‌کنید به نمایش درآیند. بخش Custom Views به شما امکان می‌دهد که فیلترها را برای استفاده آینده ذخیره کنید. هر فیلتر ذخیره‌شده یک Custom View است.



برای ساخت یک Custom View روی گزینه Create Custom View در منوی Action کلیک کنید.



در پنجره‌ای که به نمایش در می‌آید گزینه‌های موردنظرتان را انتخاب کنید.

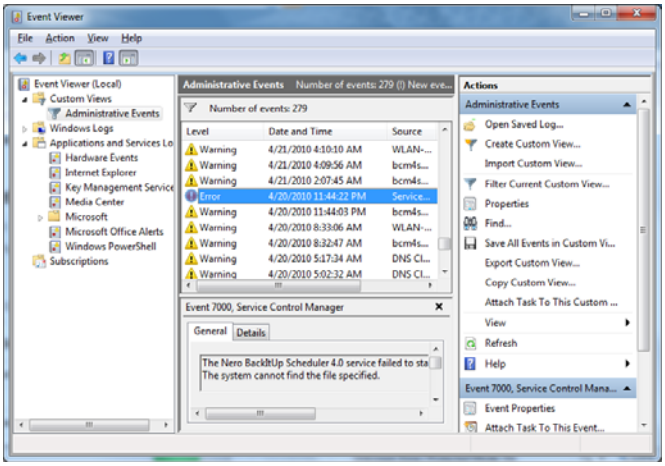


مسئله را ردیابی کنید

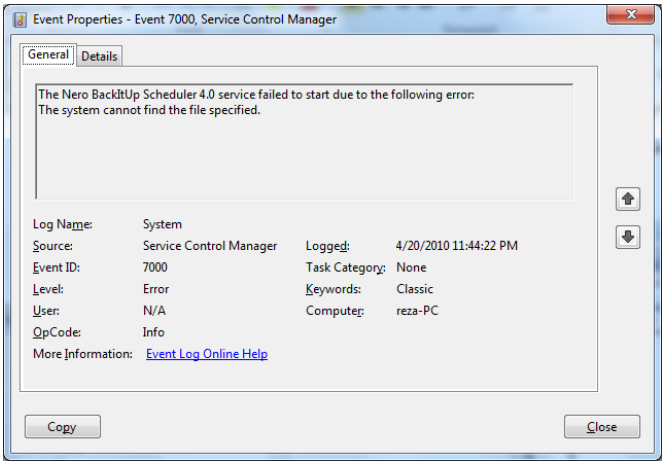
حال که می‌دانید که چگونه رویدادها را در **ویندوز۷** ردیابی کنید، در استفاده از کامپیوتر آرامش خاطر خواهید داشت. یادگیری روش‌های رفع‌اشکال و تعمیر کامپیوتر به چوبدستی جادوگران، نبوغ اینشتین، یا لیسانس مهندسی کامپیوتر نیاز ندارد. قدرت تجزیه و تحلیل یک خطا و یافتن یک پاسخ مهم است، و فایل‌های واقعه‌نگار یک منبع اساسی در ربط‌دادن مسئله به یک راه‌حل هستند.□

یک مثال برای عیب‌یابی با استفاده از برنامه Event Viewer

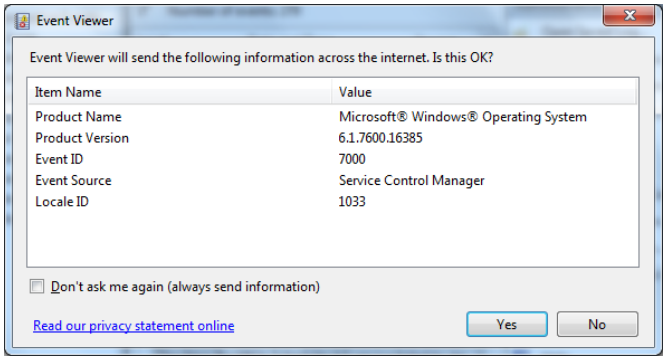
روی یک رویداد خطا کلیک-دوضرب کنید.



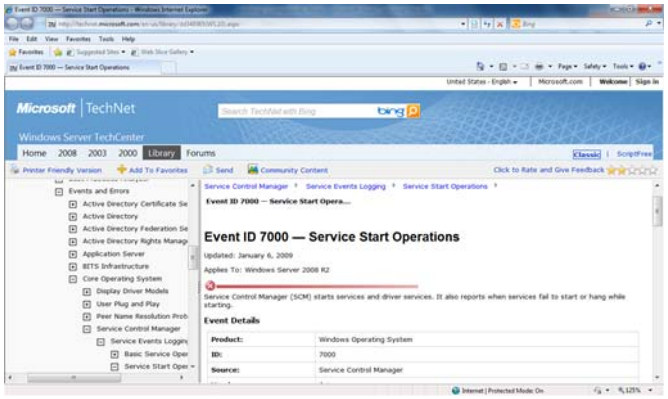
روی Event Log Online کلیک کنید.



روی Yes کلیک کنید.



اگر به اینترنت وصل باشید صفحهٔ مربوط به این خطا در سایت TechNet متعلق به مایکروسافت (http://technet.microsoft.com) باز می‌شود.



اگر توضیحی درباره آن و روش حل مسئله در بانک اطلاعاتی این سایت موجود باشد به نمایش در می‌آید.□