رفعاشکال ویندوز 7 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 شما را 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.

ویندوز ۷ هر چیزی را که در زمان بیداری روزانهٔ خودش رخ می دهد ثبت می کند، و شما می توانید این اطلاعات را برای رفع اشکال مسائل سیستم به کار بگیرید. **فایل های واقعه نگار** (log file) که **ویندوز ۷** می سازد می توانند برای حل مسائل بسیار سودمند باشند، و مایکروسافت کاری کرده است که به دست آوردن، فهمیدن، و به کار گیری این داده ها برای حل مسائل آسان شود. یک فایل واقعه نگار مانند همان جعبه سیاه کوچک بر روی یک هواپیماست، که فعالیت های **ویندوز ۷** را در زمانی که کامپیوتر در حال کار است ثبت می کند. یادگیری نحوهٔ دستیابی و فهمیدن اطلاعات فهرست شده در فایل های واقعه نگار به شما کمک خواهد کرد که یک نگاه واضح تر 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 می کند مسئلهای رخ بدهد، احتمال این که **برنامه های رانش گر** (device driver) مشکل داشته باشند زیاد است. **برنامهٔ رانش گر** یک فایل یا مجموعهای از فایل هاست که به **سیستمعامل** می گوید که چگونه با یک وسیله یا دستگاه خاص ارتباط برقرار کند. در زمان راهاندازی، **ویندوز** برای هر وسیله، از دیسک ران سی دی نویس گرفته تا صفحه کلید، یک رانش گر را بار می کند. مسائلی که در زمان راهاندازی رخ می دهند می توانند درد سرآفرین، و پیداکردن علت آنها دشوار باشد. با فعال کردن

boot logging (واقعه نگاری به هنگام عملیات بوت)، ویندوز یک فایل واقعه نگار متنی برای ثبت رانش گرهایی که در زمان راه اندازی بار می شوند و این که بارشدن آنها موفقیت آمیز یا ناموفق بوده است می سازد. ویندوز ۷ به طور خودکار این اطلاعات را به هنگامی که به حالت Safe Mode بوت کنید ذخیره می کند، اما شما معمولاً به بوت عادی به ویندوز ۷ نیاز خواهید داشت، چون حالت Safe Mode فقط رانش گرهای ضروری برای راه اندازی ویندوز را بار می کند. واقعه نگاری به هنگام عملیات بوت (boot logging) را در زمان راه اندازی به محض دیدن اولین صفحهٔ راه اندازی ویندوز ۷ با زدن کلید F8 می توانید 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.

ویندوز ۷ به بوت کردن طبیعی خود ادامه خواهد داد، و رانش گرها را برای همهٔ وسایل پیشتر نصب شده بار خواهد کرد. **ویندوز** حالا نتایج هر تلاش خود برای بارکردن یک رانش گر را در یک فایل متنی با دسترسی پذیری آسان ثبت خواهد کرد. این فایل، Ntbtlog.txt، در دیرکتوری Windows قرار دارد. **ویندوز** این اطلاعات را به یک log یا فایل واقعه نگاری پیشتر ثبت شده اضافه می کند، 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.

ເພິ້ຟີຣາເເຕັອ

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 رانش گر نداشته باشد، فایل واقعهنگار بوت در ردیابی علت مسئله به شما کمک نخواهد کرد. **ویندوز** یک برنامهٔ قدرتمندتر به نام شما کمک نخواهد که پیوسته اطلاعات مهمی را ثبت میکند که ممکن است در ردیابی علت مسئله به شما کمک کنند.

بر نامهٔ 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 کادر جستجوی منوی در Start پیدا کنید.

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



پوشهٔ Windows Logs

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

ntbtlog - Notepad	×
<u>F</u> ile <u>E</u> dit F <u>o</u> rmat <u>V</u> iew <u>H</u> elp	
Microsoft (R) Windows (R) Version 6.1 (Build 7600) 10 8 2009 15:43:53.500 Loaded driver \SystemRoot\system32\ntoskrnl.exe Loaded driver \SystemRoot\system32\halmacpi.dll	•
Loaded driver \SystemRoot\system32\kdcom.dll Loaded driver \SystemRoot\system32\mcupdate_AuthenticAM Loaded driver \SystemRoot\system32\PSHED.dll	C
Loaded driver \SystemRoot\system32\CLFS.SYS Loaded driver \SystemRoot\system32\CLFS.SYS Loaded driver \SystemRoot\system32\drivers\Wdf01000.sys	
Loaded driver \SystemRoot\system32\drivers\WDFLDR.SYS Loaded driver \SystemRoot\system32\DRIVERS\ACPI.sys Loaded driver \SystemRoot\system32\DRIVERS\WMILIB.SYS	
Loaded driver \SystemRoot\system32\DRIVERS\msisadrv.sys Loaded driver \SystemRoot\system32\DRIVERS\pci.sys Loaded driver \SystemRoot\system32\DRIVERS\vdrvroot.sys	Ŧ
٩ ا	at

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 **ویندوز۲** خود بوت کنید، و از System Recovery Options برای دیدن این فایل بهره بگیرید.

🚺 Syster	m Recovery Options	×
Choos	e a recovery tool	
Operati	ing system: Microsoft Windows on (C:) Local Disk	
1	Startup Repair	
	Automatically fix problems that are preventing Windows from starting	
	System Restore	
No.	Restore Windows to an earlier point in time	
2	System Image Recovery	
1	Recover your computer using a system image you created earlier	
	Windows Memory Diagnostic	
Titler	Check your computer for memory hardware errors	
CON.	Command Prompt	
	Open a command prompt window	
	Shut Down Restart	

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 رانش گر بار نشده است، علت می تواند یکی از موارد زیر باشد: آن فایل حذف شده است، خراب شده است، وابسته به رانش گر دیگری است که به طور موفق بار نشده است، یا طوری میزان شده است که طبق درخواست یک رانش گر دیگر به طور دستی بار شود. همچنین ممکن است که دستگاه مربوط به آن فایل رانش گر در بخش Device Manager که رانش گرها را از نو نصب، روز آمد یا فعال کنید تا مسئله حل شود.

• Application این گروه حاوی رویدادهایی است که در برنامههای کاربردی شما رخ میدهند. به عنوان مثال، یک رویداد برنامه کاربردی می تواند یک تغییر در پیکربندی، یک فایل گمشده، یا یک ارتباط راهدور قطع شده 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 می کند. به عنوان مثال، عیب در یک رانش گر یا یک برنامه سیستمی دیگر که لازم است در زمان راهاندازی ویندوز بار شوند در این بخش ثبت می شود.

• ForwardedEvents برای ذخیره رویدادهای مربوط به کامپیوترهای راه دور به کار میرود. برای جمع آوری 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.

File Action Yiew Help						
Event Viewer (Local)	Setup Number	of events: 5			Actions	
Custom Views Custom Views Aphication Setup System Paplications and Services Lo Subscriptions	Level Information Information Information Information Information Information Information Information	Date and Time 4/18/2010 10:13:27 PM 4/18/2010 10:09:46 PM 4/18/2010 10:09:44 PM 4/18/2010 10:09:34 PM 4/18/2010 10:06:50 PM	Source Servicing WUSA WUSA Servicing Servicing	E	Setup Open Saved Log Y Create Custom View Import Custom View Clear Log Y Filter Current Log D Properties We Find	•
	e Event 2, Servicing General Detai	m J	3	•	Save All Events As Attach a Task To this Log View Refresh	,
< <u> </u>	Package K89	8211 was successfully chan	ged to the I		Event 2, Servicing Event Properties Attach Task To This Event Coov	,

• 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 آمنیتی** (Security) همهٔ رویدادهایی را ثبت میکند که به سیاستهای امنیتی مربوط است. رویدادهای امنیتی، مانند دستیابی فایل و ساخت فایل، Iogonهای کاربری، و تغییرات سیاست، در اینجا به

نمایش در خواهند آمد. به طور پیش گزیده (default)، واقعهنگاری امنیتی در **ویندوز ۷** فعال نمی شود. 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 دستیایی و به کارگیری خود فایل های واقعهنگار توجه خواهیم کرد.

Event Viewer			_ @ <mark>_</mark> X
Eile Action View Help			
🛃 Event Viewer (Local)	Security Number of events: 2,072	2	Actions
Custom Views	Keywor Date and Time	Source Event *	Security
Administrate Events Administrate Events Administrate Events Application Security Setup System Forwarded Events Applications and Services Lo Subscriptions	Q. Audi 5/5/2010 406-38 AM Q. Audi 5/5/2010 406-38 AM Q. Audi 5/5/2010 406-37 AM Q. Audi 5/5/2010 326-33 AM Q. Audi 5/5/2010 32-342 AM Q. Audi 5/5/2010 32-242 AM	Micros	Open Saved Log Create Custom View Import Custom View Cleat Log Fitter Current Log Poperties Find Swe All Events As
	Event 4634, Microsoft Windows sec	urity auditing. X	View +
	General Details	A	C Refresh
	An account was logged off. Subject:		Event 4634, Microsoft Windows s Event Properties Attach Task To This Event
	1		Bin Copy

پوشه Applications and Services Logs

بخش Applications and Services Logs یک گروه جدید از رویدادهایی است که ثبت می شود. این بخش رویدادهای مربوط به برنامههای کاربردی ای را که ممکن است اثر سیستمی نداشته باشند ثبت می کند.

ile Action View Help	Applications and Camileas Lon		_	Anton
Cutom Views Totom Views Administrative Events Windows Load Services Lo Aprovent Events Internet Explorer Key Management Service Key Management Service Media Center Microsoft Office Alerts Windows DeverShell Subscriptions	Name Hardware Events Internet Explorer Key Management Service Meicrosoft Microsoft Microsoft Office Alerts Windows PowerShell	Type Administrative Administrative Administrative Administrative Administrative	Number of E 0 0 0 0 15 0	Applications and Services Logs Open Saved Log Create Custom View Import Custom View View Refresh Help Hardware Events Open Properties Help

این گروه حاوی چهارگونه رویداد است: Admin، Operational، Admin، 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 پیش فرض 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 میکند.

•رویدادهای Operational

رویدادهای Operational برای تجزیه و تحلیل و تشخیص یک مسئله یا رویداد به کار برده می شوند. یک مثال از رویدادهای Operational وصل شدن 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 رفع اشکال بر اساس این مشخصهها

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

<u>Level</u> 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 warning Information :برنامههای کاربردی ممکن است رخ بدهد: Failure Audit.

رویدادهای اطلاعاتی (Information events) عملیاتی را ثبت
 میکنند که به طور موفق به اجرا درمی آیند، مانند سرویس هایی که
 راهاندازی می شوند 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 موفقیت آمیز یک برنامه کاربردی، یا شروع به کار یک سرویس.

•رویدادهای هشداردهنده (Warning events)، که با یک نماد زرد علامت گذاری می شوند، مشخص می کنند که ویندوز در اجرای یک تکلیف سردر گمی هایی داشته است، اما خودش می توانسته است با مسئله کنار بیاید. این نوع رویدادها علائم موشکافانهای هستند که نشان می دهند یک جای کار ایراد دارد و می تواند به مسئله بینجامد.

•رویدادهای خطا (Error events) نشان می دهند که یک خطای اساسی رخ داده است و ویندوز نمی تواند مسئله را تصحیح کند. این خطاها، که با نماد ترس آور قرمز علامت گذاری می شوند، نشان می دهند که چیزی درست کار نمی کند و این که مسئله در حال حاضر روی کامپیوتر شما اثر گذار است.

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

System Number of events: 37,724 (!) New events available								
Level	Date and Time	Source	Event ID	Task Cat	-			
Error	ق.ظ 04/13/2010 10:16:16	Disk	11	None	=			
🛕 Warning	ق.ظ 04/13/2010 10:14:52	DNS Client Events	1014	None				
 Information 	ق.ظ 04/13/2010 10:14:33	Service Control M	7036	None				
 Information 	ق.ظ 04/13/2010 10:14:32	RasMan	20267	None	-			
•				•				

ົດສົ່ງແວກິທັງ

😸 Event Properties -	Event 11, Disk			×
General Details	d a controller error on	\Device\Harddisk	1\DR1.	
Log Name: Source: Event ID: Level: User: OpCode: More Information:	System Disk 11 Error N/A <u>Event Log Online</u>	Logged: Task Category: Keywords: Computer:	04/13/2010 10:16:17 None Classic Reza-PC	
Сору			C	lose

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 جستجو گر محبوب خود میتوانید یک پاسخ عمومی به دست بیاورید.

Item Name	Value
Product Name	Microsoft® Windows® Operating Sys.
Product Version	6.1.7600.16385
Event ID	11
Event Source	Disk
Locale ID	1065

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 راهحل های خود را در جایی در اینترنت ثبت کرده باشد زیاد است. **خبرگروهها** (newsgroup) و انجمن های پشتیبانی در اینترنت مکان های بسیار خوبی برای این نوع اطلاعات هستند، و درخواست کمک، به یقین، 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 فایل های واقعهنگار را پاک کنید. منوی Action به شما امکان ود گیری موفق (Success Audit) به دستیابی امنیتی موفق اشاره دارد، مانند ورود به سیستم، در حالی که رد گیری ناموفق (Failure Audit) به رویدادهایی مانند عدم موفقیت در دستیابی یک دیسکیران دلالت دارد.

Security Num	nber of ev	rents: 14,060			
Keywords	Date	Source	Event ID	Task Category	*
🔒 Audit Failure	04/13	Microsoft Windows sec	4625	Logon	H
🔒 Audit Failure	04/13	Microsoft Windows sec	4625	Logon	
🔒 Audit Failure	04/13	Microsoft Windows sec	4625	Logon	
Audit Succ	04/13	Microsoft Windows sec	4689	Process Term	
Audit Succ	04/13	Microsoft Windows sec	4689	Process Term	
Audit Succ	04/13	Microsoft Windows sec	4688	Process Creat	-

<u>Source</u>. نرمافزاری که رویداد را ثبت کرده است، که می تواند نام یک برنامه، مانند SQL Server یا بخشی از سیستم یا یک برنامه بزرگ باشد، مانند نام یک رانش گر.

Event ID. شماره معرفی کننده نوع یک رویداد.

عيبيابي

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 مرتب کردن رویدادها، روی عنوان ستون میدانی که میخواهید مرتب کنید کلیک کنید.

اگر golها حاوی مقادیر زیادی از داده ها 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 دریافته ایم که فیلتر کردن رویدادها براساس زمان و تاریخ بسیار سودمند است، زیرا یک خط زمانی دیجیتالی از فعالیت های سیستم به هنگام یک دورهٔ زمانی مشخص شده را فراهم می سازد.

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.

خواهد داد که فایل های واقعه نگار را ذخیره، باز، صادر، و پاک کنید. اگر در کامپیوتر خود زیاد با مسئله برخورد می کنید، یا دوست دارید که از واقعه نگار خود آرشیو تهیه کنید، آنها را پیش از پاک کردن در یک فایل ذخیره کنید. به هنگام ذخیرهٔ یک فایل واقعه نگار، تاریخ روز را در نام فایل بگنجانید تا بعدها در صورت نیاز به آسانی بتوانید آن را بازیابی کنید. فایل های واقعه نگار ذخیره شده را فقط با باز کردن در برنامهٔ Event Viewer می توان به نمایش در آورد، اما یک فایل واقعه نگار را در یک فایل متنی نیز می توانید ذخیره کنید تا بتوانید در برنامههای واژه پرداز مانند Notepad نیز آنها را تماشا کنید. ذخیرهٔ فایل واقعه نگار به صورت متنی، نه تنها به شما امکان خواهد داد که واقعه های خطا را ایمیل یا چاپ کنید، بلکه به شما اجازه خواهد داد که دادهها را برای انتقال از طریق اینترنت، cut

برای ساخت یک Custom View روی گزینه Create Custom View کلیک کنید.

Open Saved Log Create Custom View	6.15			_	
Import Custom View	soft-IE	_			Actions
Pafrash		Туре	Number of Events	Size	Microsoft-IE
Norman	ignostic	Analytic	N/A	0 Bytes	Open Saved Log
Help	·				Treate Custom View
Key Management Service	_				Import Custom View
Media Center					View
Microsoft					Q Refresh
Microsoft Office Alerts					Help
Windows PowerShell					
Diagnostic					Diagnostic
Microsoft-IEFRAME					Open
Diagnostic					Properties
Subscriptions					Help

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 می آورد که رویدادهای مربوط به منابعی که شما مشخص می کنید به نمایش در آیند. بخش Custom Views به شما امکان می دهد که فیلترها را برای استفاده آینده ذخیره کنید. هر فیلتر ذخیره شده یک Custom View است.

Event Viewer (Local)	Administrative	Events Number of events:	277	Actions
Custom Views	V Number	of events: 277		Administrative Events
Windows Logs Applications and Services Lo	Level Error Er	Date and Time 5/5/2010 12:42:14 AM 5/5/2010 12:42:13 AM 5/5/2010 12:42:13 AM 5/5/2010 12:42:13 AM 5/6/2010 12:42:13 AM 5/4/2010 11:56:16 PM 5/4/2010 11:56:15 PM 5/4/2010 11:56:13 PM	Source Disk Disk Disk Disk Disk Disk Kernel Kernel Kernel	Open Saved Log Create Custom View Import Custom View Filter Current Custom View Filter Current Custom View Find Save All Events in Custom VI Export Custom View Copy Custom View Attach Task To This Custom View
	The driver of	tails detected a controller error on	\Device\Hard	Refresh Help Event 11 Dick

را	موردنظرتان	گزینههای	می آید	در	نمايش	به	که	در پنجرهای	
								انتخاب كنيد.	

Create Custom Viev	
Filter XML	
Logged:	Last hour
Event level:	Critical <u>W</u> arning Ver <u>b</u> ose
	Error Information
By log	Event logs:
By source	Event sources:
Includes/Exclude exclude criteria,	es Eve <u>n</u> t IDs: Enter ID numbers and/or ID ranges separated by commas. To type a minus sign first. For example 1,3,5-99,-76 <all event="" ids=""></all>
<u>T</u> ask category:	
Keywords:	
<u>U</u> ser:	<all users=""></all>
Com <u>p</u> uter(s):	<all computers=""></all>
	Cle <u>a</u> r
	OK Cancel

مسئله را ردیابی کنید

حال که میدانید که چگونه رویدادها را در **ویندوز ۷** 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 فایل های 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.

Event Viewer (Local)	Administrative	Events Number of events:	279 (!) New eve	Act	ions	
Custom Views Administrative Events	✓ Number of events: 279			Administrative Events		
Windows Logs Applications and Services Lo Applications and Services Lo Applications and Services Lo Applications Internet Explorer Kedware Events Media Center Media Center Microsoft Microsoft Office Alerts Windows PowerShell Subscriptions	Level A Warning Warning Warning Error M Warning Warning Warning Warning Warning	Date and Time 4/21/2010 4:10:10 AM 4/21/2010 4:09:56 AM 4/21/2010 2:07:45 AM 4/20/2010 11:44:22 PM 4/20/2010 11:44:32 PM 4/20/2010 3:3:06 AM 4/20/2010 3:3:247 AM 4/20/2010 3:2:347 AM	Source WLAN bcm4s bcm4s bcm4s WLAN bcm4s DNS CL	 ✓ ✓	Open Saved Log Create Custom View Import Custom View Filter Custom View Properties Find Save All Events in Custom Vi Export Custom View	
	Event 7000, Sen	rice Control Manager	, ×		Copy Custom View Attach Task To This Custom View	
	General Det	General Details			Refresh Help	
	The system	cannot find the file specified.		Eve	nt 7000, Service Control Mana A Event Properties	

روی Event Log Online کلیک کنید.

The Nero BackItU The system canno	o Scheduler 4.0 service failed t find the file specified.	to start due to the	following error:	
Log Na <u>m</u> e: <u>S</u> ource:	System Service Control Manager	Logge <u>d</u> :	4/20/2010 11:44:22 PM	•
<u>E</u> vent ID:	7000 Error	Task Category:	None	
User:	N/A	Computer:	reza-PC	
 OpCode:	Info			
More Information:	Event Log Online Help			

روى Yes كليك كنيد.

vent Viewer will send the followin	g information across the internet. Is this OK?
tem Name	Value
Product Name	Microsoft® Windows® Operating System
Product Version	6.1.7600.16385
vent ID	7000
vent Source	Service Control Manager
.ocale ID	1033
	d information)

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

باز میشود.

C Form 10 7000 - Service Start Operations - Windows Internet I	apilone -	NAME OF TAXABLE PARTY.	and the second	CO(0)
N http://technol.microsoft.com/an-us/library/20	MERENWS20 aver		• 2 4 × 3 14	p •
File Edit View Pavorites Tools Help				
👷 Favorites 🛛 🎪 🐑 Supported Sites • 🛞 Web Sites Safety	•			
35 Event 10 7000 - Service Start Operations			S · D · D · rep. •	Salety = Tools = @ = "
			United States - English + Microsoft.com	Wekome Sign in
<i>Microsoft</i> TechNet	Search Techtod with B	ing bing 🔯		Real Contraction
			ESERTER STR	SKIX-
Home 2008 2003 2000 Library	Forums		(CL	assid ScriptFree
🖕 Printer Friendly Version 🔶 Add To Favorites	Send Kommunity (Content	Click to Rate and Give Fee	stack www.stack
Events and Brows Active Deectory Certificate Se Active Deectory Certificate Se Active Deectory Rederation Se Active Deectory Rederation Se Active Deectory Rights Manage Application Server	Event ID 7000 - Service S Event ID 7000 - Updated: January 6, 2009	- Service Start Operatio	ns	
El an a subattroccura Cree Operating System Daptay Driver Models User Plug and Play Per Name Resolution Prob Service Cantol Manager	Apples To: Windows Server	2008 RZ	also reports when services fail to start o	ir hang while
Ent's Invation/curv Core Operating System Display Driver Models User Play and Play Prer Name Resolution Prob Service Events Loggin Service Events Loggin	Apples To: Windows Server	2208 KZ M) starts services and driver services. It Windows Operating System	also reports when services fail to start o	ir hang while
Ent's IndetEncativ Core Operating System Display Driver Models User Plag and Play Feer Haam Resolution Prod Service Central Manager Service Venets Logger Essec Service Oper	Apples To: Windows Server : Service Control Manager (SC) starting. Event Details Product: ID:	2008 KZ M) starts services and driver services. It Windows Operating System 7000	also reports when services fail to start o	ir hang while

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