[illegible] Event Viewer [illegible] [illegible] [illegible] (Event Log) [illegible] [illegible]

[illegible] Event Viewer [illegible].

[illegible] [illegible]

[illegible] 10 [illegible]

[illegible]

Application Log

[illegible]

Security Log

[illegible]

System Log

[illegible]

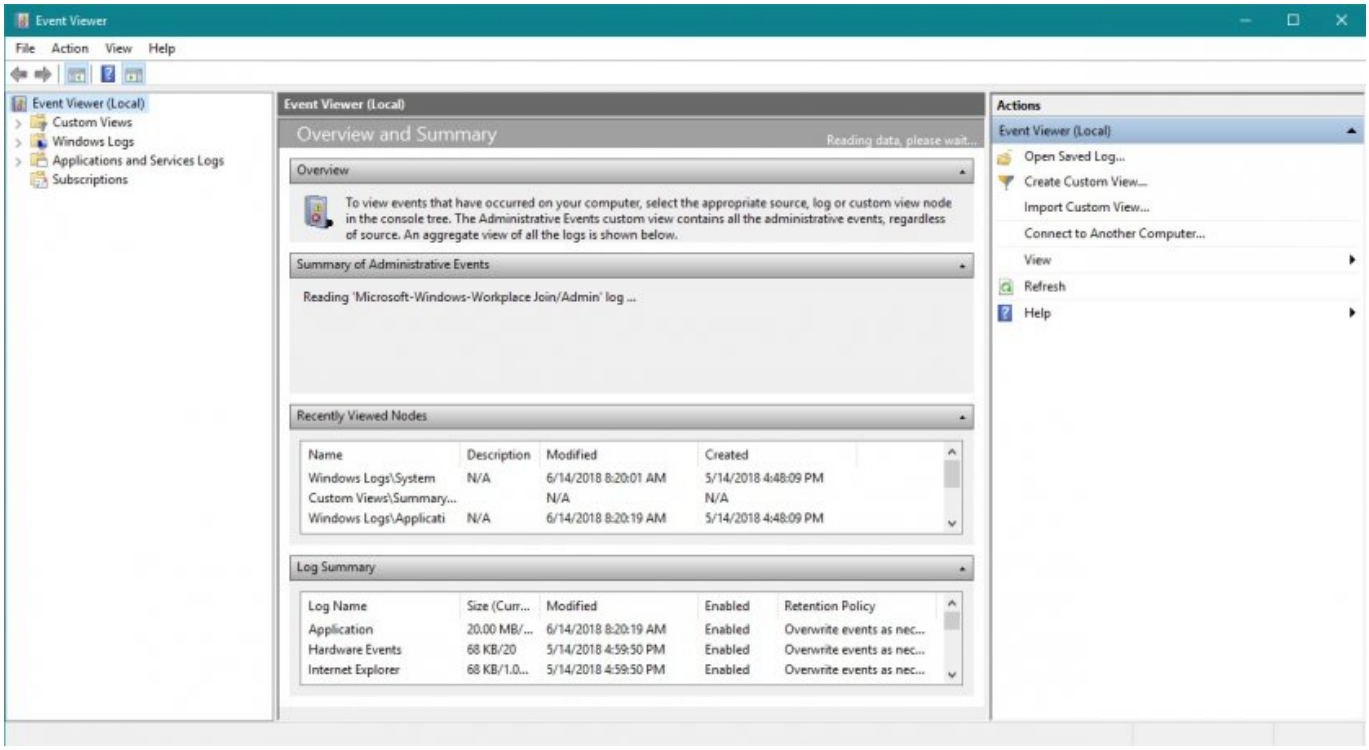
[illegible] Windows Logs [illegible] Event Viewer [illegible]

[illegible]

[illegible] 10 [illegible] Event Viewer [illegible]

[illegible] Event Viewer [illegible]

[illegible] Overview [illegible]



Summary of Administrator Events

[illegible]

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

[illegible]

Recently Viewed Nodes

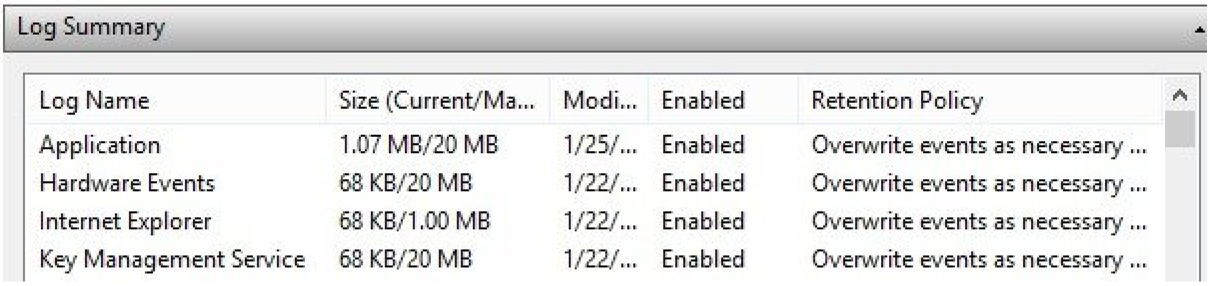
[illegible]

Log Summery

[illegible] View Events in this log [illegible]

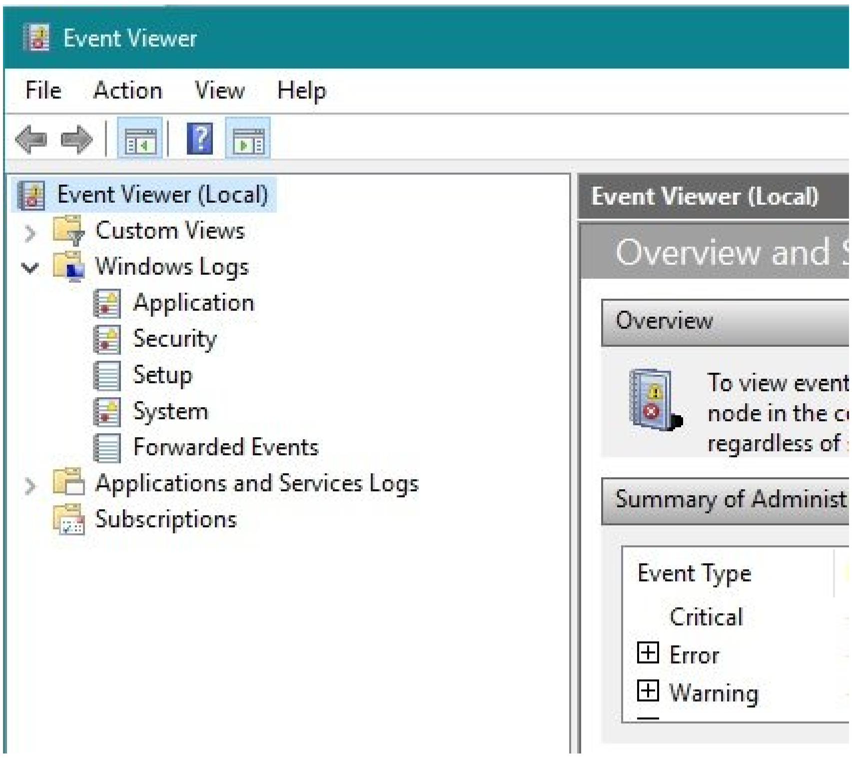
[illegible]

[illegible] Event Viewer [illegible] (Event Viewer(Local [illegible]



[illegible] Windows Logs [illegible] Application/Security/System [illegible] Windows Logs [illegible] evxt [illegible] Application [illegible] Application [illegible] SystemRoot%\System32\Winevt\Logs\Application.evtx% [illegible]

[illegible]



[illegible] Custom Views [illegible] Event Viewer [illegible]

نشان داده میشود .

Event Viewer
File
Action
View
Help
Event Viewer (Local)
Custom Views
Windows Logs
Application
Security
Setup
System
Forwarded Events
Applications and Services Logs
Subscriptions
Application
Number of events: 16,254 (!) New events available
Event 16384, Security-SPP
General
Details

Level	Date and Time	Source	Event ID	Task Category
Information	7/1/2018 3:02:36 PM	Security-SPP	1003	None
Information	7/1/2018 3:02:36 PM	Security-SPP	1003	None
Information	7/1/2018 3:02:35 PM	Security-SPP	8230	None
Information	7/1/2018 3:02:34 PM	Security-SPP	1040	None
Information	7/1/2018 3:02:33 PM	Security-SPP	16394	None
Information	7/1/2018 2:54:04 PM	DisplayFusionService	0	None
Information	7/1/2018 2:54:01 PM	DisplayFusionService	0	None
Information	7/1/2018 1:36:01 PM	DisplayFusionService	0	None
Information	7/1/2018 1:36:01 PM	ESENT	916	General
Information	7/1/2018 1:35:55 PM	ESENT	916	General

Successfully scheduled Software Protection service for re-start at 2018-07-02T10:32:12Z. Reason: RulesEngine.

اطلاعات ارائه شده از سوی این گزینه به دو گروه تقسیم شده و به کاربر نشان داده میشود . در بالای پنجره رویدادها بهمراه 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 .

نویسنده :
حمیدرضا تائبی
دسته بندی:
کارگاه
تاریخ انتشار :
11:20 - 22/08/1397
برچسب:
Event Viewer - عیب یابی سیستم - عیب یابی_سامانه تحت_شبکه - ابزار Event Viewer - مشاهده رویدادهای امنیتی - مدیریت_سیستم ویندوزی - مدیریت_ویندوز 10

نشانی
□□□□: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