ETW

Tracing done right

Siarhei Shchahrykovich

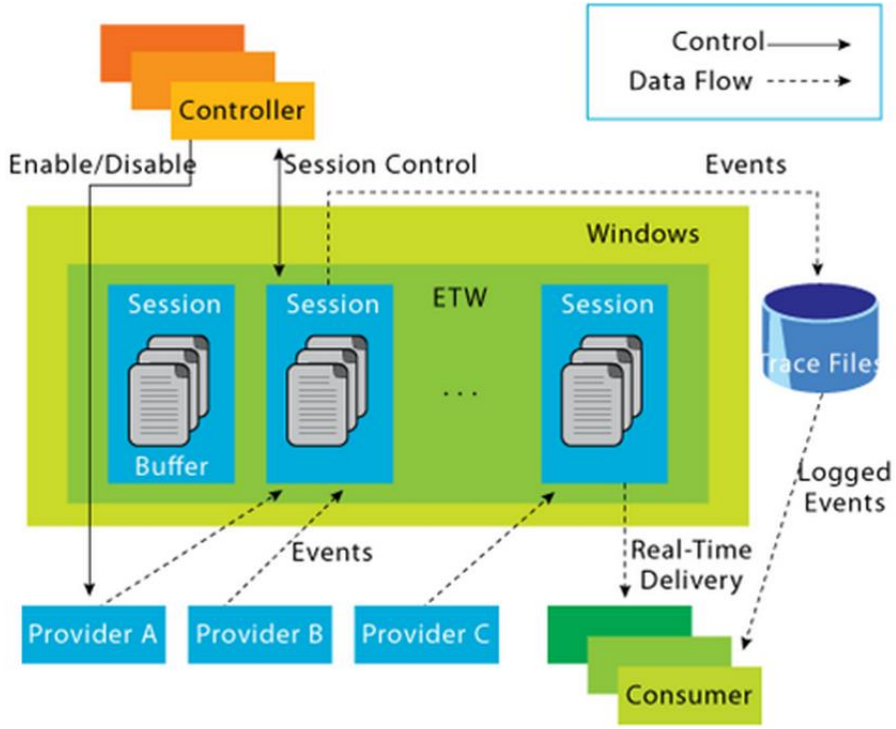
Advantages

- Primary tracing mechanism in Windows
- All Windows components support ETW
- 10k events per second < 5% CPU
- Semantic Logging (strongly-typed logging)

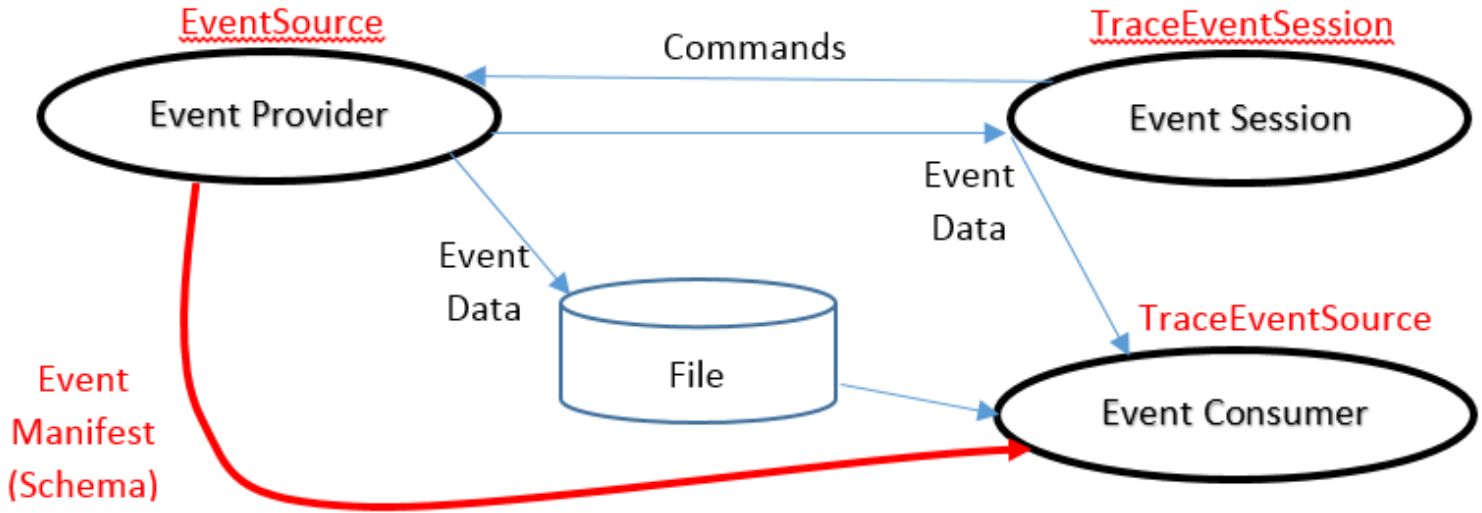
ETW in the wild

- MS SQL server
- Visual Studio
- PerfView (Download Center)
- Logging Application Block (Enterprise library) / Nlog
- IIS
- IE11
- SysInternals tools (Sysinternals Suite)
- Windows Performance Toolkit (ADK, WDK, SDK)
- Microsoft Message Analyzer

Architecture



ETW and .Net


EventSource
Commands
TraceEventSession
Event Provider
Event Session
Event
Data
Event
Data
TraceEventSource
File
Event
Manifest
(Schema)
Event Consumer

ETW Providers

- 976 Windows providers (logman query providers)
- 98 Chrome providers (logman query providers -pid 1000)
- .Net Common Language Runtime (GC, Thread Pool, Interop, JIT, Loader and etc)
- node-etw and Windows ETW and Perf Counters to Node.js
- Microsoft-Windows-HttpService (Http.sys)
- Microsoft-Windows-IIS-W3SVC

Samples

- WPT
- PerfView
- Custom diagnostic tool

Summary

- High performance
- Full support in .Net
- Windows 8+/ Windows Phone / Windows RT
- Good tool support
- Requires admin rights

shchegrikovich@gmail.com