
Composants

AB – v1.21 (20/09/2022)

ETW

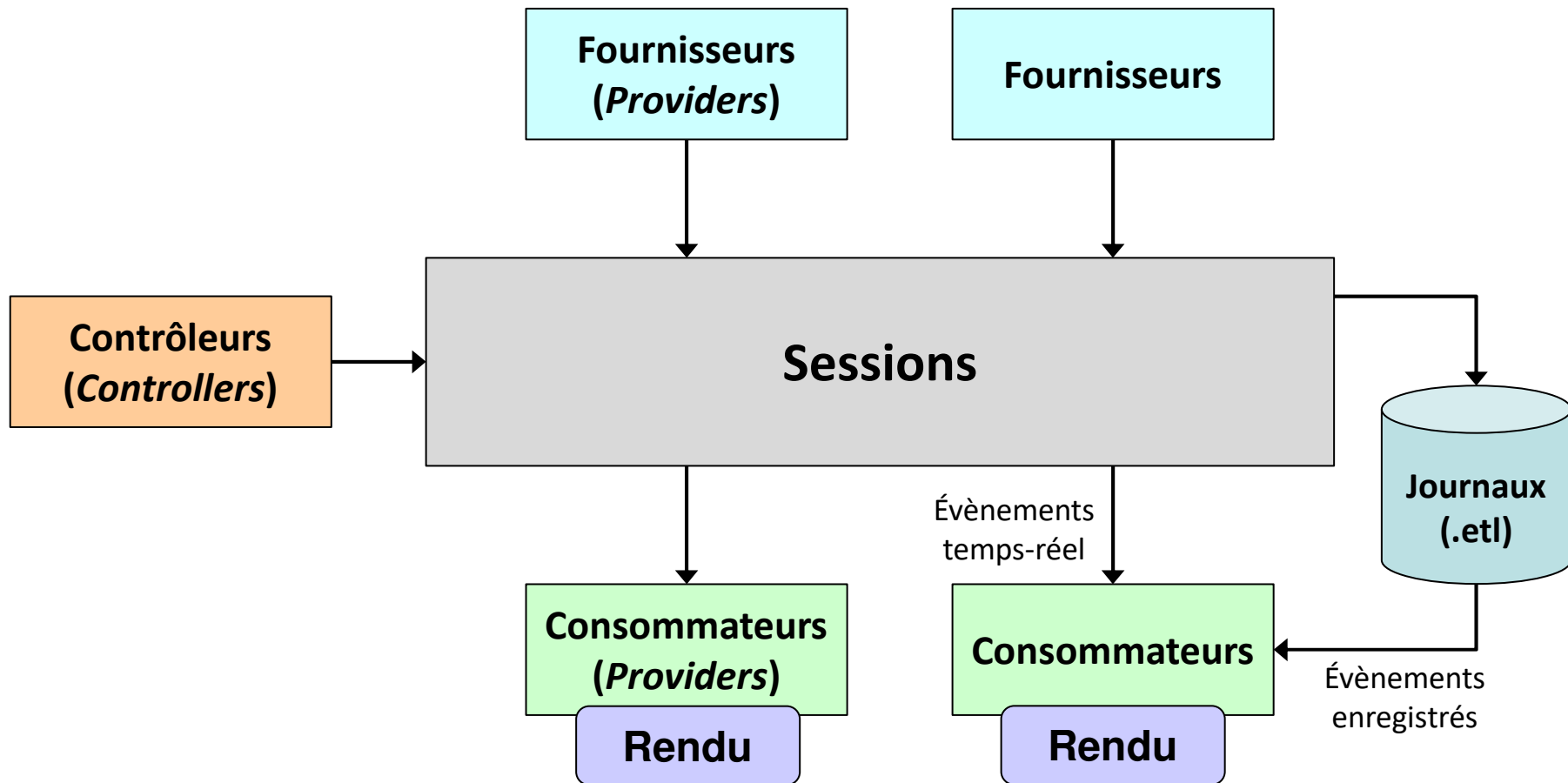
Event Tracing for Windows

ETW

Event Tracing for Windows

- Mécanisme de gestion de traces d'événements associées à des sessions
- Disponible pour les applications et les pilotes noyaux

ETW



Fournisseurs

- **MOF (Classic) providers :**
 - Évènements décrits dans un fichier MOF (*Managed Object Format*) publié dans le *namespace* root\wmi
- **Manifest-based providers :**
 - Évènements décrits dans un *instrumentation manifest* (format XML), généralement inclus dans un binaire
- **WPP providers :**
 - Évènements intégrés au code via des macro WPP et stockés dans un fichier TMF (Trace Message Format) et généralement stockés dans les symboles privés
- **TraceLogging providers :**
 - Évènements intégrés au code et rendus sans manifeste (métadonnées incluses avec l'évènement)

TraceLogging providers

<https://learn.microsoft.com/en-us/windows/win32/tracelogging/tracelogging-native-quick-start>

```
#include <TraceLoggingProvider.h> // The C/C++ TraceLogging API

TRACELOGGING_DECLARE_PROVIDER(g_hTraceProvider);
TRACELOGGING_DEFINE_PROVIDER(
    g_hTraceProvider, "SampleProvier",
    (0x0205c616,0xcf97,0x5c11,0x97,0x56,0x56,0xa2,0xce,0xe0,0x2c,0xa7)    // {0205c616-cf97-5c11-9756-56a2cee02ca7}
);

void main()
{
    char sampleValue[] = "Sample value";

    // Register the provider
    TraceLoggingRegister(g_hTraceProvider);

    // Log an event
    TraceLoggingWrite(g_hTraceProvider,                          // handle to provider
        "HelloWorldTestEvent",                                   // Event Name that should uniquely identify your event.
        TraceLoggingValue(sampleValue, "TestMessage")           // Field for your event in the form of (value, field name).
    );

    // Stop TraceLogging and unregister the provider
    TraceLoggingUnregister(g_hTraceProvider);
}
```

TraceLogging Wrapper Macros

<https://learn.microsoft.com/en-us/windows/win32/tracelogging/tracelogging-wrapper-macros>

```
#include <winmeta.h>
TraceLoggingLevel(WINEVENT_LEVEL_VERBOSE)

#define PROVIDER_KEYWORD_TEST    0x1
TraceLoggingKeyword(PROVIDER_KEYWORD_TEST)

TraceLoggingValue
TraceLoggingBool
TraceLoggingString / TraceLoggingWideString / TraceLoggingUtf8String
TraceLoggingUInt32 / TraceLoggingHexUInt32
TraceLoggingGuid / TraceLoggingPointer / TraceLoggingSid
TraceLoggingFileTime / TraceLoggingSystemTime
TraceLoggingPointer / TraceLoggingStruct
TraceLoggingWinError / TraceLoggingNTSTATUS / TraceLoggingHRESULT
```