1833 lines (1499 loc) · 66.4 KB

Code Blame Raw

```
<Providers>
    <Provider>
        <Name>Microsoft-Windows-WindowsUpdateClient</Name>
        <Metadata>
            <Guid>{945A8954-C147-4ACD-923F-40C45405A658}</Guid>
            <ResourceFilePath>C:\Windows\system32\wuaueng.dll</ResourceFilePath>
            <ParameterFilePath>C:\Windows\system32\wuaueng.dll</ParameterFilePath>
            <MessageFilePath>C:\Windows\system32\wuaueng.dll</MessageFilePath>
            <HelpLink>https://go.microsoft.com/fwlink/events.asp?CoName=Microsoft%20Corporation&amp
            <PublisherMessage>Microsoft-Windows-WindowsUpdateClient</PublisherMessage>
            <Channels>
                <Channel>
                    <Message>System</Message>
                    <Path>System</Path>
                    <Index>0</Index>
                    <Id>8</Id>
                    <Imported>true</Imported>
                </Channel>
                <Channel>
                    <Message></Message>
                    <Path>Microsoft-Windows-WindowsUpdateClient/Operational</Path>
                    <Index>1</Index>
                    <Id>16</Id>
                    <Imported>false</Imported>
```

```
                </Channel>
                <Channel>
                    <Message></Message>
                    <Path>Microsoft-Windows-WindowsUpdateClient/Analytic</Path>
                    <Index>2</Index>
                    <Id>17</Id>
                    <Imported>false</Imported>
                </Channel>
            </Channels>
            <Levels>
                <Level>
                    <Message>Error</Message>
                    <Name>win:Error</Name>
                    <Value>2</Value>
                </Level>
                <Level>
                    <Message>Warning</Message>
                    <Name>win:Warning</Name>
                    <Value>3</Value>
                </Level>
                <Level>
                    <Message>Information</Message>
                    <Name>win:Informational</Name>
                    <Value>4</Value>
                </Level>
            </Levels>
            <Tasks>
                <Task>
                    <Message>Windows Update Agent</Message>
                    <Name>Agent</Name>
                    <Value>1</Value>
                </Task>
                <Task>
                    <Message>Automatic Updates</Message>
                    <Name>AU</Name>
                    <Value>2</Value>
                </Task>
            </Tasks>
            <Opcodes>
                <Opcode>
                    <Message>Info</Message>
                    <Name>win:Info</Name>
                    <Value>0</Value>
                    <Task>0</Task>
                </Opcode>
                <Opcode>
```

```
71                      <Message>Start</Message>
72                      <Name>win:Start</Name>
73                      <Value>1</Value>
74                      <Task>0</Task>
75                  </Opcode>
76                  <Opcode>
77                      <Message>Stop</Message>
78                      <Name>win:Stop</Name>
79                      <Value>2</Value>
80                      <Task>0</Task>
81                  </Opcode>
82                  <Opcode>
83                      <Message>SelfUpdate</Message>
84                      <Name>selfupdate</Name>
85                      <Value>10</Value>
86                      <Task>0</Task>
87                  </Opcode>
88                  <Opcode>
89                      <Message>Check for Updates</Message>
90                      <Name>detect</Name>
91                      <Value>11</Value>
92                      <Task>0</Task>
93                  </Opcode>
94                  <Opcode>
95                      <Message>Download</Message>
96                      <Name>download</Name>
97                      <Value>12</Value>
98                      <Task>0</Task>
99                  </Opcode>
100                 <Opcode>
101                     <Message>Installation</Message>
102                     <Name>install</Name>
103                     <Value>13</Value>
104                     <Task>0</Task>
105                 </Opcode>
106                 <Opcode>
107                     <Message>Uninstallation</Message>
108                     <Name>uninstall</Name>
109                     <Value>14</Value>
110                     <Task>0</Task>
111                 </Opcode>
112                 <Opcode>
113                     <Message>Reboot</Message>
114                     <Name>reboot</Name>
115                     <Value>15</Value>
```

```
117                     </Opcode>
```

EVTX-ETW-Resources/ETWProvidersManifests/Windows10/1903/W10_1903_Pro_20200714_18362.959/WEPExplorer/Microsoft-Windows-WindowsUpdateClient.xml at f1b010ce0ee1b71e3024180de1a3e67f99701fe4 · nasbench/EVTX-ETW-Resources · GitHub - 31/10/2024 16:00 https://github.com/nasbench/EVTX-ETW-Resources/blob/f1b010ce0ee1b71e3024180de1a3e67f99701fe4/ETWProvidersManifests/Windows10/1903/W10_1903_Pro_2
Windows-WindowsUpdateClient.xml

EVTX-ETW-Resources/ETWProvidersManifests/Windows10/1903/W10_1903_Pro_20200714_18362.959/WEPExplorer/Microsoft-Windows-WindowsUpdateClient.xml at f1b010ce0ee1b71e3024180de1a3e67f99701fe4 · nasbench/EVTX-ETW-Resources · GitHub - 31/10/2024 16:00 https://github.com/nasbench/EVTX-ETW-Resources/blob/f1b010ce0ee1b71e3024180de1a3e67f99701fe4/ETWProvidersManifests/Windows10/1903/W10_1903_Pro_2
Windows-WindowsUpdateClient.xml

EVTX-ETW-Resources/ETWProvidersManifests/Windows10/1903/W10_1903_Pro_20200714_18362.959/WEPExplorer/Microsoft-Windows-WindowsUpdateClient.xml at f1b010ce0ee1b71e3024180de1a3e67f99701fe4 · nasbench/EVTX-ETW-Resources · GitHub - 31/10/2024 16:00 https://github.com/nasbench/EVTX-ETW-Resources/blob/f1b010ce0ee1b71e3024180de1a3e67f99701fe4/ETWProvidersManifests/Windows10/1903/W10_1903_Pro_2
Windows-WindowsUpdateClient.xml

EVTX-ETW-Resources/ETWProvidersManifests/Windows10/1903/W10_1903_Pro_20200714_18362.959/WEPExplorer/Microsoft-Windows-WindowsUpdateClient.xml at f1b010ce0ee1b71e3024180de1a3e67f99701fe4 · nasbench/EVTX-ETW-Resources · GitHub - 31/10/2024 16:00 https://github.com/nasbench/EVTX-ETW-Resources/blob/f1b010ce0ee1b71e3024180de1a3e67f99701fe4/ETWProvidersManifests/Windows10/1903/W10_1903_Pro_2
Windows-WindowsUpdateClient.xml

EVTX-ETW-Resources/ETWProvidersManifests/Windows10/1903/W10_1903_Pro_20200714_18362.959/WEPExplorer/Microsoft-Windows-WindowsUpdateClient.xml at f1b010ce0ee1b71e3024180de1a3e67f99701fe4 · nasbench/EVTX-ETW-Resources · GitHub - 31/10/2024 16:00 https://github.com/nasbench/EVTX-ETW-Resources/blob/f1b010ce0ee1b71e3024180de1a3e67f99701fe4/ETWProvidersManifests/Windows10/1903/W10_1903_Pro_2
Windows-WindowsUpdateClient.xml

EVTX-ETW-Resources/ETWProvidersManifests/Windows10/1903/W10_1903_Pro_20200714_18362.959/WEPExplorer/Microsoft-Windows-WindowsUpdateClient.xml at f1b010ce0ee1b71e3024180de1a3e67f99701fe4 · nasbench/EVTX-ETW-Resources · GitHub - 31/10/2024 16:00 https://github.com/nasbench/EVTX-ETW-Resources/blob/f1b010ce0ee1b71e3024180de1a3e67f99701fe4/ETWProvidersManifests/Windows10/1903/W10_1903_Pro_2
Windows-WindowsUpdateClient.xml

EVTX-ETW-Resources/ETWProvidersManifests/Windows10/1903/W10_1903_Pro_20200714_18362.959/WEPExplorer/Microsoft-Windows-WindowsUpdateClient.xml at f1b010ce0ee1b71e3024180de1a3e67f99701fe4 · nasbench/EVTX-ETW-Resources · GitHub - 31/10/2024 16:00 https://github.com/nasbench/EVTX-ETW-Resources/blob/f1b010ce0ee1b71e3024180de1a3e67f99701fe4/ETWProvidersManifests/Windows10/1903/W10_1903_Pro_2
Windows-WindowsUpdateClient.xml

EVTX-ETW-Resources/ETWProvidersManifests/Windows10/1903/W10_1903_Pro_20200714_18362.959/WEPExplorer/Microsoft-Windows-WindowsUpdateClient.xml at f1b010ce0ee1b71e3024180de1a3e67f99701fe4 · nasbench/EVTX-ETW-Resources · GitHub - 31/10/2024 16:00 https://github.com/nasbench/EVTX-ETW-Resources/blob/f1b010ce0ee1b71e3024180de1a3e67f99701fe4/ETWProvidersManifests/Windows10/1903/W10_1903_Pro_2
Windows-WindowsUpdateClient.xml

EVTX-ETW-Resources/ETWProvidersManifests/Windows10/1903/W10_1903_Pro_20200714_18362.959/WEPExplorer/Microsoft-Windows-WindowsUpdateClient.xml at f1b010ce0ee1b71e3024180de1a3e67f99701fe4 · nasbench/EVTX-ETW-Resources · GitHub - 31/10/2024 16:00 https://github.com/nasbench/EVTX-ETW-Resources/blob/f1b010ce0ee1b71e3024180de1a3e67f99701fe4/ETWProvidersManifests/Windows10/1903/W10_1903_Pro_2
Windows-WindowsUpdateClient.xml

EVTX-ETW-Resources/ETWProvidersManifests/Windows10/1903/W10_1903_Pro_20200714_18362.959/WEPExplorer/Microsoft-Windows-WindowsUpdateClient.xml at f1b010ce0ee1b71e3024180de1a3e67f99701fe4 · nasbench/EVTX-ETW-Resources · GitHub - 31/10/2024 16:00 https://github.com/nasbench/EVTX-ETW-Resources/blob/f1b010ce0ee1b71e3024180de1a3e67f99701fe4/ETWProvidersManifests/Windows10/1903/W10_1903_Pro_2
Windows-WindowsUpdateClient.xml

EVTX-ETW-Resources/ETWProvidersManifests/Windows10/1903/W10_1903_Pro_20200714_18362.959/WEPExplorer/Microsoft-Windows-WindowsUpdateClient.xml at f1b010ce0ee1b71e3024180de1a3e67f99701fe4 · nasbench/EVTX-ETW-Resources · GitHub - 31/10/2024 16:00 https://github.com/nasbench/EVTX-ETW-Resources/blob/f1b010ce0ee1b71e3024180de1a3e67f99701fe4/ETWProvidersManifests/Windows10/1903/W10_1903_Pro_2
Windows-WindowsUpdateClient.xml

EVTX-ETW-Resources/ETWProvidersManifests/Windows10/1903/W10_1903_Pro_20200714_18362.959/WEPExplorer/Microsoft-Windows-WindowsUpdateClient.xml at f1b010ce0ee1b71e3024180de1a3e67f99701fe4 · nasbench/EVTX-ETW-Resources · GitHub - 31/10/2024 16:00 https://github.com/nasbench/EVTX-ETW-Resources/blob/f1b010ce0ee1b71e3024180de1a3e67f99701fe4/ETWProvidersManifests/Windows10/1903/W10_1903_Pro_2
Windows-WindowsUpdateClient.xml

EVTX-ETW-Resources/ETWProvidersManifests/Windows10/1903/W10_1903_Pro_20200714_18362.959/WEPExplorer/Microsoft-Windows-WindowsUpdateClient.xml at f1b010ce0ee1b71e3024180de1a3e67f99701fe4 · nasbench/EVTX-ETW-Resources · GitHub - 31/10/2024 16:00 https://github.com/nasbench/EVTX-ETW-Resources/blob/f1b010ce0ee1b71e3024180de1a3e67f99701fe4/ETWProvidersManifests/Windows10/1903/W10_1903_Pro_2
Windows-WindowsUpdateClient.xml

EVTX-ETW-Resources/ETWProvidersManifests/Windows10/1903/W10_1903_Pro_20200714_18362.959/WEPExplorer/Microsoft-Windows-WindowsUpdateClient.xml at f1b010ce0ee1b71e3024180de1a3e67f99701fe4 · nasbench/EVTX-ETW-Resources · GitHub - 31/10/2024 16:00 https://github.com/nasbench/EVTX-ETW-Resources/blob/f1b010ce0ee1b71e3024180de1a3e67f99701fe4/ETWProvidersManifests/Windows10/1903/W10_1903_Pro_2
Windows-WindowsUpdateClient.xml

EVTX-ETW-Resources/ETWProvidersManifests/Windows10/1903/W10_1903_Pro_20200714_18362.959/WEPExplorer/Microsoft-Windows-WindowsUpdateClient.xml at f1b010ce0ee1b71e3024180de1a3e67f99701fe4 · nasbench/EVTX-ETW-Resources · GitHub - 31/10/2024 16:00 https://github.com/nasbench/EVTX-ETW-Resources/blob/f1b010ce0ee1b71e3024180de1a3e67f99701fe4/ETWProvidersManifests/Windows10/1903/W10_1903_Pro_2
Windows-WindowsUpdateClient.xml

EVTX-ETW-Resources/ETWProvidersManifests/Windows10/1903/W10_1903_Pro_20200714_18362.959/WEPExplorer/Microsoft-Windows-WindowsUpdateClient.xml at f1b010ce0ee1b71e3024180de1a3e67f99701fe4 · nasbench/EVTX-ETW-Resources · GitHub - 31/10/2024 16:00 https://github.com/nasbench/EVTX-ETW-Resources/blob/f1b010ce0ee1b71e3024180de1a3e67f99701fe4/ETWProvidersManifests/Windows10/1903/W10_1903_Pro_2
Windows-WindowsUpdateClient.xml

EVTX-ETW-Resources/ETWProvidersManifests/Windows10/1903/W10_1903_Pro_20200714_18362.959/WEPExplorer/Microsoft-Windows-WindowsUpdateClient.xml at f1b010ce0ee1b71e3024180de1a3e67f99701fe4 · nasbench/EVTX-ETW-Resources · GitHub - 31/10/2024 16:00 https://github.com/nasbench/EVTX-ETW-Resources/blob/f1b010ce0ee1b71e3024180de1a3e67f99701fe4/ETWProvidersManifests/Windows10/1903/W10_1903_Pro_2
Windows-WindowsUpdateClient.xml

EVTX-ETW-Resources/ETWProvidersManifests/Windows10/1903/W10_1903_Pro_20200714_18362.959/WEPExplorer/Microsoft-Windows-WindowsUpdateClient.xml at f1b010ce0ee1b71e3024180de1a3e67f99701fe4 · nasbench/EVTX-ETW-Resources · GitHub - 31/10/2024 16:00 https://github.com/nasbench/EVTX-ETW-Resources/blob/f1b010ce0ee1b71e3024180de1a3e67f99701fe4/ETWProvidersManifests/Windows10/1903/W10_1903_Pro_2
Windows-WindowsUpdateClient.xml

EVTX-ETW-Resources/ETWProvidersManifests/Windows10/1903/W10_1903_Pro_20200714_18362.959/WEPExplorer/Microsoft-Windows-WindowsUpdateClient.xml at f1b010ce0ee1b71e3024180de1a3e67f99701fe4 · nasbench/EVTX-ETW-Resources · GitHub - 31/10/2024 16:00 https://github.com/nasbench/EVTX-ETW-Resources/blob/f1b010ce0ee1b71e3024180de1a3e67f99701fe4/ETWProvidersManifests/Windows10/1903/W10_1903_Pro_2
Windows-WindowsUpdateClient.xml

EVTX-ETW-Resources/ETWProvidersManifests/Windows10/1903/W10_1903_Pro_20200714_18362.959/WEPExplorer/Microsoft-Windows-WindowsUpdateClient.xml at f1b010ce0ee1b71e3024180de1a3e67f99701fe4 · nasbench/EVTX-ETW-Resources · GitHub - 31/10/2024 16:00 https://github.com/nasbench/EVTX-ETW-Resources/blob/f1b010ce0ee1b71e3024180de1a3e67f99701fe4/ETWProvidersManifests/Windows10/1903/W10_1903_Pro_2
Windows-WindowsUpdateClient.xml

EVTX-ETW-Resources/ETWProvidersManifests/Windows10/1903/W10_1903_Pro_20200714_18362.959/WEPExplorer/Microsoft-Windows-WindowsUpdateClient.xml at f1b010ce0ee1b71e3024180de1a3e67f99701fe4 · nasbench/EVTX-ETW-Resources · GitHub - 31/10/2024 16:00 https://github.com/nasbench/EVTX-ETW-Resources/blob/f1b010ce0ee1b71e3024180de1a3e67f99701fe4/ETWProvidersManifests/Windows10/1903/W10_1903_Pro_2
Windows-WindowsUpdateClient.xml

EVTX-ETW-Resources/ETWProvidersManifests/Windows10/1903/W10_1903_Pro_20200714_18362.959/WEPExplorer/Microsoft-Windows-WindowsUpdateClient.xml at f1b010ce0ee1b71e3024180de1a3e67f99701fe4 · nasbench/EVTX-ETW-Resources · GitHub - 31/10/2024 16:00 https://github.com/nasbench/EVTX-ETW-Resources/blob/f1b010ce0ee1b71e3024180de1a3e67f99701fe4/ETWProvidersManifests/Windows10/1903/W10_1903_Pro_2
Windows-WindowsUpdateClient.xml

EVTX-ETW-Resources/ETWProvidersManifests/Windows10/1903/W10_1903_Pro_20200714_18362.959/WEPExplorer/Microsoft-Windows-WindowsUpdateClient.xml at f1b010ce0ee1b71e3024180de1a3e67f99701fe4 · nasbench/EVTX-ETW-Resources · GitHub - 31/10/2024 16:00 https://github.com/nasbench/EVTX-ETW-Resources/blob/f1b010ce0ee1b71e3024180de1a3e67f99701fe4/ETWProvidersManifests/Windows10/1903/W10_1903_Pro_2
Windows-WindowsUpdateClient.xml

EVTX-ETW-Resources/ETWProvidersManifests/Windows10/1903/W10_1903_Pro_20200714_18362.959/WEPExplorer/Microsoft-Windows-WindowsUpdateClient.xml at f1b010ce0ee1b71e3024180de1a3e67f99701fe4 · nasbench/EVTX-ETW-Resources · GitHub - 31/10/2024 16:00 https://github.com/nasbench/EVTX-ETW-Resources/blob/f1b010ce0ee1b71e3024180de1a3e67f99701fe4/ETWProvidersManifests/Windows10/1903/W10_1903_Pro_2
Windows-WindowsUpdateClient.xml

EVTX-ETW-Resources/ETWProvidersManifests/Windows10/1903/W10_1903_Pro_20200714_18362.959/WEPExplorer/Microsoft-Windows-WindowsUpdateClient.xml at f1b010ce0ee1b71e3024180de1a3e67f99701fe4 · nasbench/EVTX-ETW-Resources · GitHub - 31/10/2024 16:00 https://github.com/nasbench/EVTX-ETW-Resources/blob/f1b010ce0ee1b71e3024180de1a3e67f99701fe4/ETWProvidersManifests/Windows10/1903/W10_1903_Pro_2
Windows-WindowsUpdateClient.xml

EVTX-ETW-Resources/ETWProvidersManifests/Windows10/1903/W10_1903_Pro_20200714_18362.959/WEPExplorer/Microsoft-Windows-WindowsUpdateClient.xml at f1b010ce0ee1b71e3024180de1a3e67f99701fe4 · nasbench/EVTX-ETW-Resources · GitHub - 31/10/2024 16:00 https://github.com/nasbench/EVTX-ETW-Resources/blob/f1b010ce0ee1b71e3024180de1a3e67f99701fe4/ETWProvidersManifests/Windows10/1903/W10_1903_Pro_2
Windows-WindowsUpdateClient.xml

EVTX-ETW-Resources/ETWProvidersManifests/Windows10/1903/W10_1903_Pro_20200714_18362.959/WEPExplorer/Microsoft-Windows-WindowsUpdateClient.xml at f1b010ce0ee1b71e3024180de1a3e67f99701fe4 · nasbench/EVTX-ETW-Resources · GitHub - 31/10/2024 16:00 https://github.com/nasbench/EVTX-ETW-Resources/blob/f1b010ce0ee1b71e3024180de1a3e67f99701fe4/ETWProvidersManifests/Windows10/1903/W10_1903_Pro_2
Windows-WindowsUpdateClient.xml

```
1426                    <Channel>System</Channel>
1427                    <Level>Information</Level>
1428                    <Task>Windows Update Agent</Task>
1429                    <Opcode>Revert</Opcode>
1430                    <Keyword>Success Revert</Keyword>
1431                    <Message><![CDATA[
1432    Revert Successful: Windows successfully reverted the following update: %1]]></Message>
1433                    <Template><![CDATA[
1434    <template xmlns="http://schemas.microsoft.com/win/2004/08/events">
1435      <data name="updateTitle" inType="win:UnicodeString" outType="xs:string"/>
1436      <data name="updateGuid" inType="win:GUID" outType="xs:GUID"/>
1437      <data name="updateRevisionNumber" inType="win:UInt32" outType="xs:unsignedInt"/>
1438      <data name="serviceGuid" inType="win:GUID" outType="xs:GUID"/>
1439    </template>
1440    ]]></Template>
1441                </Event>
1442                <Event>
1443                    <Id>213</Id>
1444                    <Version>0</Version>
```

```
                    <Channel>System</Channel>
                    <Level>Error</Level>
                    <Task>Windows Update Agent</Task>
                    <Opcode>Revert</Opcode>
                    <Keyword>Failure Revert</Keyword>
                    <Message><![CDATA[
    Revert Failure: Windows failed to revert the following update with error %1: %2]]></Message>
                    <Template><![CDATA[
    <template xmlns="http://schemas.microsoft.com/win/2004/08/events">
      <data name="errorCode" inType="win:HexInt32" outType="win:HexInt32"/>
      <data name="updatelist" inType="win:UnicodeString" outType="xs:string"/>
      <data name="updateGuid" inType="win:GUID" outType="xs:GUID"/>
      <data name="updateRevisionNumber" inType="win:UInt32" outType="xs:unsignedInt"/>
    </template>
    ]]></Template>
                </Event>
                <Event>
                    <Id>214</Id>
                    <Version>0</Version>
                    <Channel>System</Channel>
                    <Level>Information</Level>
                    <Task>Windows Update Agent</Task>
                    <Opcode>Revert</Opcode>
                    <Keyword>Started Revert</Keyword>
                    <Message><![CDATA[
    Revert Started: Windows has started reverting the following update: %1]]></Message>
                    <Template><![CDATA[
    <template xmlns="http://schemas.microsoft.com/win/2004/08/events">
      <data name="updateTitle" inType="win:UnicodeString" outType="xs:string"/>
      <data name="updateGuid" inType="win:GUID" outType="xs:GUID"/>
      <data name="updateRevisionNumber" inType="win:UInt32" outType="xs:unsignedInt"/>
    </template>
    ]]></Template>
                </Event>
                <Event>
                    <Id>215</Id>
                    <Version>0</Version>
                    <Channel>System</Channel>
                    <Level>Information</Level>
                    <Task>Windows Update Agent</Task>
                    <Opcode>Uninstallation</Opcode>
                    <Keyword>Started Uninstallation</Keyword>
                    <Message><![CDATA[
    Uninstallation started: Windows has started uninstallnig the following update: %1]]></Message>
                    <Template><![CDATA[
```

```
1491        <data name="updateTitle" inType="win:UnicodeString" outType="xs:string"/>
1492        <data name="updateGuid" inType="win:GUID" outType="xs:GUID"/>
1493        <data name="updateRevisionNumber" inType="win:UInt32" outType="xs:unsignedInt"/>
1494      </template>
1495      ]]></Template>
1496                  </Event>
1497              </EventMetadata>
1498          </Provider>
1499      </Providers>
```