



Sign in

nasbench / EVTX-ETW-Resources

Public

Notifications

Fork 68

Star 344

Code

Issues 4

Pull requests

Actions

Projects

Security

Insights

EVTX-ETW-Resources / ETWProvidersManifests / Windows10 / 1903
/ W10_1903_Pro_20200714_18362.959 / WEPEXplorer
/ Microsoft-Windows-WindowsUpdateClient.xml



1833 lines (1499 loc) · 66.4 KB

Code

Blame

Raw



```
1     <Providers>
2         <Provider>
3             <Name>Microsoft-Windows-WindowsUpdateClient</Name>
4             <Metadata>
5                 <Guid>{945A8954-C147-4ACD-923F-40C45405A658}</Guid>
6                 <ResourceFilePath>C:\Windows\system32\wuaueng.dll</ResourceFilePath>
7                 <ParameterFilePath>C:\Windows\system32\wuaueng.dll</ParameterFilePath>
8                 <MessageFilePath>C:\Windows\system32\wuaueng.dll</MessageFilePath>
9                 <HelpLink>https://go.microsoft.com/fwlink/events.asp?CoName=Microsoft%20Corporation&amp;CoProduct=Windows%20Update%20Client</HelpLink>
10                <PublisherMessage>Microsoft-Windows-WindowsUpdateClient</PublisherMessage>
11                <Channels>
12                    <Channel>
13                        <Message>System</Message>
14                        <Path>System</Path>
15                        <Index>0</Index>
16                        <Id>8</Id>
17                        <Imported>true</Imported>
18                    </Channel>
19                    <Channel>
20                        <Message></Message>
21                        <Path>Microsoft-Windows-WindowsUpdateClient/Operational</Path>
22                        <Index>1</Index>
23                        <Id>16</Id>
24                        <Imported>false</Imported>
```

```
25         </Channel>
26     </Channel>
27     <Message></Message>
28     <Path>Microsoft-Windows-WindowsUpdateClient/Analytic</Path>
29     <Index>2</Index>
30     <Id>17</Id>
31     <Imported>>false</Imported>
32 </Channel>
33 </Channels>
34 <Levels>
35     <Level>
36         <Message>Error</Message>
37         <Name>win:Error</Name>
38         <Value>2</Value>
39     </Level>
40     <Level>
41         <Message>Warning</Message>
42         <Name>win:Warning</Name>
43         <Value>3</Value>
44     </Level>
45     <Level>
46         <Message>Information</Message>
47         <Name>win:Informational</Name>
48         <Value>4</Value>
49     </Level>
50 </Levels>
51 <Tasks>
52     <Task>
53         <Message>Windows Update Agent</Message>
54         <Name>Agent</Name>
55         <Value>1</Value>
56     </Task>
57     <Task>
58         <Message>Automatic Updates</Message>
59         <Name>AU</Name>
60         <Value>2</Value>
61     </Task>
62 </Tasks>
63 <Opcodes>
64     <Opcode>
65         <Message>Info</Message>
66         <Name>win:Info</Name>
67         <Value>0</Value>
68         <Task>0</Task>
69     </Opcode>
70 </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>
```

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_20200714_18362.959/WEPEXplorer/Microsoft-Windows-WindowsUpdateClient.xml		
117	</Opcode>	


```
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>
```



```
1445         <Channel>System</Channel>
1446         <Level>Error</Level>
1447         <Task>Windows Update Agent</Task>
1448         <Opcode>Revert</Opcode>
1449         <Keyword>Failure Revert</Keyword>
1450         <Message><![CDATA[
1451 Revert Failure: Windows failed to revert the following update with error %1: %2]]></Message>
1452         <Template><![CDATA[
1453 <template xmlns="http://schemas.microsoft.com/win/2004/08/events">
1454     <data name="errorCode" inType="win:HexInt32" outType="win:HexInt32"/>
1455     <data name="updatelist" inType="win:UnicodeString" outType="xs:string"/>
1456     <data name="updateGuid" inType="win:GUID" outType="xs:GUID"/>
1457     <data name="updateRevisionNumber" inType="win:UInt32" outType="xs:unsignedInt"/>
1458 </template>
1459 ]]></Template>
1460     </Event>
1461     <Event>
1462         <Id>214</Id>
1463         <Version>0</Version>
1464         <Channel>System</Channel>
1465         <Level>Information</Level>
1466         <Task>Windows Update Agent</Task>
1467         <Opcode>Revert</Opcode>
1468         <Keyword>Started Revert</Keyword>
1469         <Message><![CDATA[
1470 Revert Started: Windows has started reverting the following update: %1]]></Message>
1471         <Template><![CDATA[
1472 <template xmlns="http://schemas.microsoft.com/win/2004/08/events">
1473     <data name="updateTitle" inType="win:UnicodeString" outType="xs:string"/>
1474     <data name="updateGuid" inType="win:GUID" outType="xs:GUID"/>
1475     <data name="updateRevisionNumber" inType="win:UInt32" outType="xs:unsignedInt"/>
1476 </template>
1477 ]]></Template>
1478     </Event>
1479     <Event>
1480         <Id>215</Id>
1481         <Version>0</Version>
1482         <Channel>System</Channel>
1483         <Level>Information</Level>
1484         <Task>Windows Update Agent</Task>
1485         <Opcode>Uninstallation</Opcode>
1486         <Keyword>Started Uninstallation</Keyword>
1487         <Message><![CDATA[
1488 Uninstallation started: Windows has started uninstalnig the following update: %1]]></Message>
1489         <Template><![CDATA[
1490 <template xmlns="http://schemas.microsoft.com/win/2004/08/events">
```

```
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>
```