

Product

Solutions

Resources

Open Source

Enterprise

Pricing

Sign in

Sign up

nasbench

/

EVTX-ETW-Resources

Public

Notifications

Fork

68

Star

344

<> Code

Issues

4

Pull requests

Actions

Projects

Security

Insights

Files

f1b010c

Go to file

> .github

> ETWEventsList

> ETWProvidersCSVs

> ETWProvidersManifests

> ThirdParty

> Windows10

> 1507

> 1511

> 1607

> 1703

> 1709

> 1803

> 1809

> 1903

> 1909

> 2004

> 20H2

> 21H1

> 21H2

> 22H2

> W10\_22H2\_Pro\_20221115\_1...

> W10\_22H2\_Pro\_20221220\_1...

> W10\_22H2\_Pro\_20230117\_1...

> W10\_22H2\_Pro\_20230221\_1...

> W10\_22H2\_Pro\_20230321\_1...

All.xml

Application Popup.xml

Application-Addon-Event-P...

Error Instrument.xml

Intel-iaLPSS-GPIO.xml

Intel-iaLPSS-I2C.xml

Intel-iaLPSS2-GPIO2.xml

Intel-iaLPSS2-I2C.xml

LsaSrv.xml

Microsoft-Antimalware-AM...

Microsoft-Antimalware-Engi...

EVTX-ETW-Resources / ETWProvidersManifests / Windows10 / 22H2 / W10\_22H2\_Pro\_20230321\_19045.2728 / WEPEXplorer / LsaSrv.xml

AndrewRathbun

add March 2023 ISOs

3e09319 · last year

History

Code

Blame

1345 lines (977 loc) · 43.8 KB

Raw

1 <Providers>

2 <Provider>

3 <Name>LsaSrv</Name>

4 <Metadata>

5 <Guid>{199FE037-2B82-40A9-82AC-E1D46C792B99}</Guid>

6 <ResourceFilePath>C:\Windows\System32\lsasrv.dll</ResourceFilePath>

7 <ParameterFilePath></ParameterFilePath>

8 <MessageFilePath>C:\Windows\System32\lsasrv.dll</MessageFilePath>

9 <HelpLink>https://go.microsoft.com/fwlink/events.asp?CoName=Microsoft%20Cor

10 <PublisherMessage>Microsoft-Windows-LSA</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-LSA/Performance</Path>

22 <Index>1</Index>

23 <Id>16</Id>

24 <Imported>>false</Imported>

25 </Channel>

26 <Channel>

27 <Message>Operational</Message>

28 <Path>Microsoft-Windows-LSA/Operational</Path>

29 <Index>2</Index>

30 <Id>17</Id>

31 <Imported>>false</Imported>

32 </Channel>

33 <Channel>

34 <Message>Diagnostic</Message>

35 <Path>Microsoft-Windows-LSA/Diagnostic</Path>

36 <Index>3</Index>

37 <Id>18</Id>

38 <Imported>>false</Imported>

39 </Channel>

40 </Channels>

41 <Levels>

42 <Level>

43 <Message>Critical</Message>

44 <Name>win:Critical</Name>

45 <Value>1</Value>

46 </Level>

47 <Level>

48 <Message>Error</Message>

49 <Name>win:Error</Name>

50 <Value>2</Value>

51 </Level>

52 <Level>

53 <Message>Warning</Message>

54 <Name>win:Warning</Name>

Page 1 of 14

<div><div></div><div>Microsoft-Antimalware-Engi...</div></div>	55	<div>&lt;Value&gt;3&lt;/Value&gt;</div>
<div><div></div><div>Microsoft-Antimalware-NIS...</div></div>	56	<div>&lt;/Level&gt;</div>
<div><div></div><div>Microsoft-Antimalware-Prot...</div></div>	57	<div>&lt;Level&gt;</div>
<div><div></div><div>Microsoft-Antimalware-RTP...</div></div>	58	<div>&lt;Message&gt;Information&lt;/Message&gt;</div>
<div><div></div><div>Microsoft-Antimalware-Sca...</div></div>	59	<div>&lt;Name&gt;win:Informational&lt;/Name&gt;</div>
<div><div></div><div>Microsoft-Antimalware-Serv...</div></div>	60	<div>&lt;Value&gt;4&lt;/Value&gt;</div>
	61	<div>&lt;/Level&gt;</div>
	62	<div>&lt;/Levels&gt;</div>
	63	<div>&lt;Tasks&gt;</div>
	64	<div>&lt;Task&gt;</div>
	65	<div>&lt;Message&gt;Security Package Manager&lt;/Message&gt;</div>
	66	<div>&lt;Name&gt;CATEGORY_SPM&lt;/Name&gt;</div>
	67	<div>&lt;Value&gt;1&lt;/Value&gt;</div>
	68	<div>&lt;/Task&gt;</div>
	69	<div>&lt;Task&gt;</div>
	70	<div>&lt;Message&gt;Locator&lt;/Message&gt;</div>
	71	<div>&lt;Name&gt;CATEGORY_LOCATOR&lt;/Name&gt;</div>
	72	<div>&lt;Value&gt;2&lt;/Value&gt;</div>
	73	<div>&lt;/Task&gt;</div>
	74	<div>&lt;Task&gt;</div>
	75	<div>&lt;Message&gt;SPNEGO (Negotiator)&lt;/Message&gt;</div>
	76	<div>&lt;Name&gt;CATEGORY_NEGOTIATE&lt;/Name&gt;</div>
	77	<div>&lt;Value&gt;3&lt;/Value&gt;</div>
	78	<div>&lt;/Task&gt;</div>
	79	<div>&lt;Task&gt;</div>
	80	<div>&lt;Message&gt;Logon Cache&lt;/Message&gt;</div>
	81	<div>&lt;Name&gt;CATEGORY_LOGON_CACHE&lt;/Name&gt;</div>
	82	<div>&lt;Value&gt;4&lt;/Value&gt;</div>
	83	<div>&lt;/Task&gt;</div>
	84	<div>&lt;Task&gt;</div>
	85	<div>&lt;Message&gt;LSA Logon&lt;/Message&gt;</div>
	86	<div>&lt;Name&gt;CATEGORY_LSA_LOGON&lt;/Name&gt;</div>
	87	<div>&lt;Value&gt;5&lt;/Value&gt;</div>
	88	<div>&lt;/Task&gt;</div>
	89	<div>&lt;Task&gt;</div>
	90	<div>&lt;Message&gt;LSA SID-Name Lookup&lt;/Message&gt;</div>
	91	<div>&lt;Name&gt;CATEGORY_LSA_LOOKUP&lt;/Name&gt;</div>
	92	<div>&lt;Value&gt;6&lt;/Value&gt;</div>
	93	<div>&lt;/Task&gt;</div>
	94	<div>&lt;Task&gt;</div>
	95	<div>&lt;Message&gt;Max&lt;/Message&gt;</div>
	96	<div>&lt;Name&gt;CATEGORY_MAX_CATEGORY&lt;/Name&gt;</div>
	97	<div>&lt;Value&gt;7&lt;/Value&gt;</div>
	98	<div>&lt;/Task&gt;</div>
	99	<div>&lt;/Tasks&gt;</div>
	100	<div>&lt;Opcodes&gt;</div>
	101	<div>&lt;Opcode&gt;</div>
	102	<div>&lt;Message&gt;Start&lt;/Message&gt;</div>
	103	<div>&lt;Name&gt;win:Start&lt;/Name&gt;</div>
	104	<div>&lt;Value&gt;1&lt;/Value&gt;</div>
	105	<div>&lt;Task&gt;0&lt;/Task&gt;</div>
	106	<div>&lt;/Opcode&gt;</div>
	107	<div>&lt;Opcode&gt;</div>
	108	<div>&lt;Message&gt;Stop&lt;/Message&gt;</div>
	109	<div>&lt;Name&gt;win:Stop&lt;/Name&gt;</div>
	110	<div>&lt;Value&gt;2&lt;/Value&gt;</div>
	111	<div>&lt;Task&gt;0&lt;/Task&gt;</div>
	112	<div>&lt;/Opcode&gt;</div>
	113	<div>&lt;/Opcodes&gt;</div>
	114	<div>&lt;Keywords&gt;</div>
	115	<div>&lt;Keyword&gt;</div>
	116	<div>&lt;Message&gt;&lt;/Message&gt;</div>
	117	<div>&lt;Name&gt;WPDBusEnumStartTrigger&lt;/Name&gt;</div>



















--	--



```
946         </Event>
947     <Event>
948         <Id>40969</Id>
949         <Version>0</Version>
950         <Channel>System</Channel>
```

```
950         <Channel>System</Channel>
951         <Level>Information</Level>
952         <Message><![CDATA[
953     The Security System has received an authentication attempt, and determined that the pro
954         <Template><![CDATA[
955     <template xmlns="http://schemas.microsoft.com/win/2004/08/events">
956         <data name="Protocol" inType="win:UnicodeString" outType="xs:string"/>
957     </template>
958     ]]></Template>
959     </Event>
960     <Event>
961         <Id>40970</Id>
962         <Version>0</Version>
963         <Channel>System</Channel>
964         <Level>Warning</Level>
965         <Message><![CDATA[
966     The Security System has detected a downgrade attempt when contacting the 3-part SPN
967
968     %1
969
970     with error code %2. Authentication was denied.]]></Message>
971         <Template><![CDATA[
972     <template xmlns="http://schemas.microsoft.com/win/2004/08/events">
973         <data name="Target" inType="win:UnicodeString" outType="xs:string"/>
974         <data name="Error" inType="win:UnicodeString" outType="xs:string"/>
975     </template>
976     ]]></Template>
977     </Event>
978     <Event>
979         <Id>45056</Id>
980         <Version>0</Version>
981         <Channel>System</Channel>
982         <Level>Warning</Level>
983         <Message><![CDATA[
984     Logon cache was disabled. Intermittent authentication failures may result during period
985         <Template><![CDATA[
986     ]]></Template>
987     </Event>
988     <Event>
989         <Id>45057</Id>
990         <Version>0</Version>
991         <Channel>System</Channel>
992         <Level>Information</Level>
993         <Message><![CDATA[
994     A failed logon attempt has caused a logon cache entry for user %1 to be deleted. The au
995         <Template><![CDATA[
996     <template xmlns="http://schemas.microsoft.com/win/2004/08/events">
997         <data name="Username" inType="win:UnicodeString" outType="xs:string"/>
998         <data name="Package" inType="win:UnicodeString" outType="xs:string"/>
999         <data name="Error" inType="win:UnicodeString" outType="xs:string"/>
1000     </template>
1001     ]]></Template>
1002     </Event>
1003     <Event>
1004         <Id>45058</Id>
1005         <Version>0</Version>
1006         <Channel>System</Channel>
1007         <Level>Information</Level>
1008         <Message><![CDATA[
1009     A logon cache entry for user %1 was the oldest entry and was removed. The timestamp of
1010         <Template><![CDATA[
1011     <template xmlns="http://schemas.microsoft.com/win/2004/08/events">
1012         <data name="UserName" inType="win:UnicodeString" outType="xs:string"/>
1013         <data name="TimeStamp" inType="win:SYSTEMTIME" outType="xs:dateTime"/>
1014     </template>
1015     ]]></Template>
1016     </Event>
1017     </EventMetadata>
1018 </Provider>
1019 </Providers>
```