1377 lines (1003 loc) · 44.7 KB

Code Blame Raw

```
<Providers>
    <Provider>
        <Name>LsaSrv</Name>
        <Metadata>
            <Guid>{199FE037-2B82-40A9-82AC-E1D46C792B99}</Guid>
            <ResourceFilePath>%windir%\System32\lsasrv.dll</ResourceFilePath>
            <ParameterFilePath></ParameterFilePath>
            <MessageFilePath>%windir%\System32\lsasrv.dll</MessageFilePath>
            <HelpLink></HelpLink>
            <PublisherMessage>Microsoft-Windows-LSA</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-LSA/Performance</Path>
                    <Index>1</Index>
                    <Id>16</Id>
                    <Imported>false</Imported>
```

```
                </Channel>
                <Channel>
                    <Message>Operational</Message>
                    <Path>Microsoft-Windows-LSA/Operational</Path>
                    <Index>2</Index>
                    <Id>17</Id>
                    <Imported>false</Imported>
                </Channel>
                <Channel>
                    <Message>Diagnostic</Message>
                    <Path>Microsoft-Windows-LSA/Diagnostic</Path>
                    <Index>3</Index>
                    <Id>18</Id>
                    <Imported>false</Imported>
                </Channel>
            </Channels>
            <Levels>
                <Level>
                    <Message>Critical</Message>
                    <Name>win:Critical</Name>
                    <Value>1</Value>
                </Level>
                <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>Security Package Manager</Message>
                    <Name>CATEGORY_SPM</Name>
                    <Value>1</Value>
                </Task>
                <Task>
                    <Message>Locator</Message>
```

```
                    <Name>CATEGORY_LOCATOR</Name>
                    <Value>2</Value>
                </Task>
                <Task>
                    <Message>SPNEGO (Negotiator)</Message>
                    <Name>CATEGORY_NEGOTIATE</Name>
                    <Value>3</Value>
                </Task>
                <Task>
                    <Message>Logon Cache</Message>
                    <Name>CATEGORY_LOGON_CACHE</Name>
                    <Value>4</Value>
                </Task>
                <Task>
                    <Message>LSA Logon</Message>
                    <Name>CATEGORY_LSA_LOGON</Name>
                    <Value>5</Value>
                </Task>
                <Task>
                    <Message>LSA SID-Name Lookup</Message>
                    <Name>CATEGORY_LSA_LOOKUP</Name>
                    <Value>6</Value>
                </Task>
                <Task>
                    <Message>Max</Message>
                    <Name>CATEGORY_MAX_CATEGORY</Name>
                    <Value>7</Value>
                </Task>
            </Tasks>
            <Opcodes>
                <Opcode>
                    <Message>Start</Message>
                    <Name>win:Start</Name>
                    <Value>1</Value>
                    <Task>0</Task>
                </Opcode>
                <Opcode>
                    <Message>Stop</Message>
                    <Name>win:Stop</Name>
                    <Value>2</Value>
                    <Task>0</Task>
                </Opcode>
            </Opcodes>
            <Keywords>
                <Keyword>
```

```
116                     <Message></Message>
117                     <Name>WPDBusEnumStartTrigger</Name>
```

EVTX-ETW-Resources/ETWProvidersManifests/Windows11/22H2/W11_22H2_Pro_20221220_22621.963/WEPExplorer/LsaSrv.xml at 7a806a148b3d9d381193d4a80356016e6e8b1ee8 · nasbench/EVTX-ETW-Resources · GitHub - 31/10/2024 15:42
https://github.com/nasbench/EVTX-ETW-Resources/blob/7a806a148b3d9d381193d4a80356016e6e8b1ee8/ETWProvidersManifests/Windows11/22H2/W11_22H2_Pro

EVTX-ETW-Resources/ETWProvidersManifests/Windows11/22H2/W11_22H2_Pro_20221220_22621.963/WEPExplorer/LsaSrv.xml at 7a806a148b3d9d381193d4a80356016e6e8b1ee8 · nasbench/EVTX-ETW-Resources · GitHub - 31/10/2024 15:42
https://github.com/nasbench/EVTX-ETW-Resources/blob/7a806a148b3d9d381193d4a80356016e6e8b1ee8/ETWProvidersManifests/Windows11/22H2/W11_22H2_Pro

```
                    <Level>Information</Level>
                    <Message><![CDATA[
The Security System has received an authentication request directly for authentication protocol %1.
                    <Template><![CDATA[
<template xmlns="http://schemas.microsoft.com/win/2004/08/events">
  <data name="Protocol" inType="win:UnicodeString" outType="xs:string"/>
</template>
]]></Template>
                </Event>
                <Event>
                    <Id>40968</Id>
                    <Version>0</Version>
                    <Channel>System</Channel>
                    <Level>Warning</Level>
                    <Message><![CDATA[
```

```
987     The Security System has received an authentication request that could not be decoded. The request h
988                     <Template><![CDATA[
989     ]]></Template>
990                 </Event>
991                 <Event>
992                     <Id>40969</Id>
993                     <Version>0</Version>
994                     <Channel>System</Channel>
995                     <Level>Information</Level>
996                     <Message><![CDATA[
997     The Security System has received an authentication attempt, and determined that the protocol %1 is
998                     <Template><![CDATA[
999     <template xmlns="http://schemas.microsoft.com/win/2004/08/events">
1000      <data name="Protocol" inType="win:UnicodeString" outType="xs:string"/>
1001    </template>
1002    ]]></Template>
1003                </Event>
1004                <Event>
1005                    <Id>45056</Id>
1006                    <Version>0</Version>
1007                    <Channel>System</Channel>
1008                    <Level>Warning</Level>
1009                    <Message><![CDATA[
1010    Logon cache was disabled. Intermittent authentication failures may result during periods of network
1011                    <Template><![CDATA[
1012    ]]></Template>
1013                </Event>
1014                <Event>
1015                    <Id>45057</Id>
1016                    <Version>0</Version>
1017                    <Channel>System</Channel>
1018                    <Level>Information</Level>
1019                    <Message><![CDATA[
1020    A failed logon attempt has caused a logon cache entry for user %1 to be deleted. The authentication
1021                    <Template><![CDATA[
1022    <template xmlns="http://schemas.microsoft.com/win/2004/08/events">
1023      <data name="Username" inType="win:UnicodeString" outType="xs:string"/>
1024      <data name="Package" inType="win:UnicodeString" outType="xs:string"/>
1025      <data name="Error" inType="win:UnicodeString" outType="xs:string"/>
1026    </template>
1027    ]]></Template>
1028                </Event>
1029                <Event>
1030                    <Id>45058</Id>
1031                    <Version>0</Version>
```

```
1032                    <Channel>System</Channel>
1033                    <Level>Information</Level>
1034                    <Message><![CDATA[
1035    A logon cache entry for user %1 was the oldest entry and was removed. The timestamp of this entry w
1036                    <Template><![CDATA[
1037    <template xmlns="http://schemas.microsoft.com/win/2004/08/events">
1038      <data name="UserName" inType="win:UnicodeString" outType="xs:string"/>
1039      <data name="TimeStamp" inType="win:SYSTEMTIME" outType="xs:dateTime"/>
1040    </template>
1041    ]]></Template>
1042                </Event>
1043            </EventMetadata>
1044        </Provider>
1045    </Providers>
```