Cryptographic Services failed while processing the OnIdentity() call in the System Writer Object.

"Microsoft Link-Layer Discovery Protocol" binary is \Windows\system32\DRIVERS\mslldp.sys

Its config registry key is HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Services\MsLldp

During backup a VSS process running under NETWORK\_SERVICE account calls cryptcatsvc!CSystemWriter::AddLegacyDriverFiles(), which enumerates all the drivers records in Service Control Manager database and tries opening each one of them. , The function fails on MSLLDP record with "Access Denied" error.

Turned out it fails because MSLLDP driver's security permissions do not allow NETWORK\_SERVICE to access the driver record.

The binary security descriptor for the record is located here:

HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Services\MsLldp\Security

It should be modified, I used SC.EXE and Sysinternals' ACCESSCHK.EXE to fix it.

The original security descriptor looked like below:

>**accesschk.exe -c mslldp**

mslldp
  RW NT AUTHORITY\SYSTEM
  RW BUILTIN\Administrators
  RW S-1-5-32-549       <- these are server operators
  R  NT SERVICE\NlaSvc

No service account is allowed to access MSLLDP driver

The security descriptor for the drivers that were processed successfully looked this way:

>**accesschk.exe -c mup**

mup
  RW NT AUTHORITY\SYSTEM
  RW BUILTIN\Administrators
  R  NT AUTHORITY\INTERACTIVE
  R  NT AUTHORITY\SERVICE  <- this gives access to services

How to add access rights for NT AUTHORITY\SERVICE to MSLLDP service:

1. Run: **SC sdshow MSLLDP**

You'll get something like below (SDDL language is documented on MSDN):

D:(D;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BG)(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;SY)(A;;CCDCLCSWRPDTLOCRSDRCWDWO;;;BA)(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;SO)(A;;LCRPWP;;;S-1-5-80-3141615172-2057878085-1754447212-2405740020-3916490453)S:(AU;FA;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;WD)

2. Run: **SC sdshow MUP**

You'll get:

D:(A;;CCLCSWRPWPDTLOCRRC;;;SY)(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)(A;;CCLCSWLOCRRC;;;IU)(A;;CCLCSWLOCRRC;;;SU)S:(AU;FA;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;WD)

3. Take NT AUTHORITY\ SERVICE entry, which is (A;;CCLCSWLOCRRC;;;SU) and add it to the original MSLLDP security descriptor properly, right before the last S:(AU... group.

4. Apply the new security descriptor to MSLLDP service :

**sc sdset** MSLLDP D:(D;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BG)(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;SY)(A;;CCDCLCSWRPDTLOCRSDRCWDWO;;;BA)(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;SO)(A;;LCRPWP;;;S-1-5-80-3141615172-2057878085-1754447212-2405740020-3916490453)(A;;CCLCSWLOCRRC;;;SU)S:(AU;FA;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;WD)

5. Check the result:

**>accesschk.exe -c mslldp**

mslldp
  RW NT AUTHORITY\SYSTEM
  RW BUILTIN\Administrators
  RW S-1-5-32-549
  R  NT SERVICE\NlaSvc
  R  NT AUTHORITY\SERVICE