Unrecoverable Error with the VSS System Writer

https://campus.barracuda.com/doc/98224605/

Volume Shadow Copy Service (VSS) Error Message: “Encountered unrecoverable error with the VSS System Writer”

During a Physical Imaging backup, the backup agent attempts to create a snapshot of the machine and uses various snapshot providers and writers in the process.

The system VSS Writer is required to ensure that restored virtual disks are bootable when taking a snapshot backup of the boot volumes.

If the snapshot does not occur, the following error message is displayed:

"Encountered unrecoverable error with the VSS System Writer. See the event log on the target machine."

Possible Solutions

Apply one of the following solutions in the order specified to resolve the error.

Note: Not all the solutions may be required.

Task	Description
1	Ensure Volume Shadow Copy Service is running.
2	Update/Create registry DWORD key.
3	Validate Component Services permissions
4	Modify MSLLDP Driver's Security Permissions.

Task 1. Ensure Volume Shadow Copy Service Is Running

To ensure Volume Shadow Copy Service is running, perform the following steps.

1. Open Service Manager (Start –> Run –> services.msc).
2. Scroll to the Volume Shadow Copy service and ensure that it is running.
3. If Volume Shadow Copy service is not running, right click, select **Properties,** and update the execution to **Automatic** and reboot.

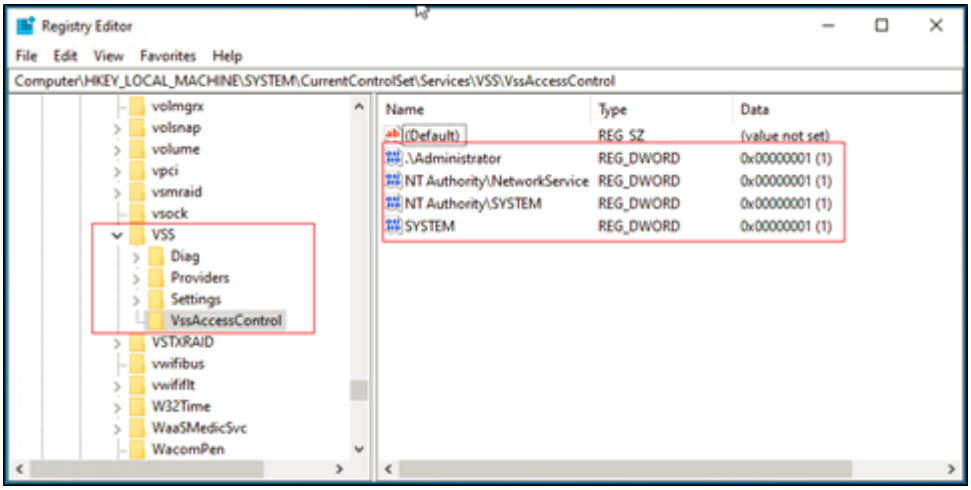
Task 2. Update/Create Registry DWORD Key

To update/create the registry DWORD key, perform the following steps.

1. Open Service Manager (Start –> Run –> services.msc).
2. Scroll to the Volume Shadow Copy service and check the log-on tab of the account used for service execution (\Administrator, Network Service, Local System).
3. Open the registry editor (Start –> Run –> regedit)
4. Navigate to HKEY_LOCAL_MACHINE>SYSTEM>CurrentControlSet>Services>VSS>VssAccessControl.
5. Create a **DWORD** key entry and assign a value of 1.

- Key name is equal to the fully qualified name of the system account being used by the Volume Shadow Copy service.
- For the .\Administrator account, use the key **.\Administrator.**
- For the Network Service account, use the key **NT Authority\NetworkService**
- For the Local System account, use the key **NT Authority\SYSTEM**.

The following image provides an example of the new settings.

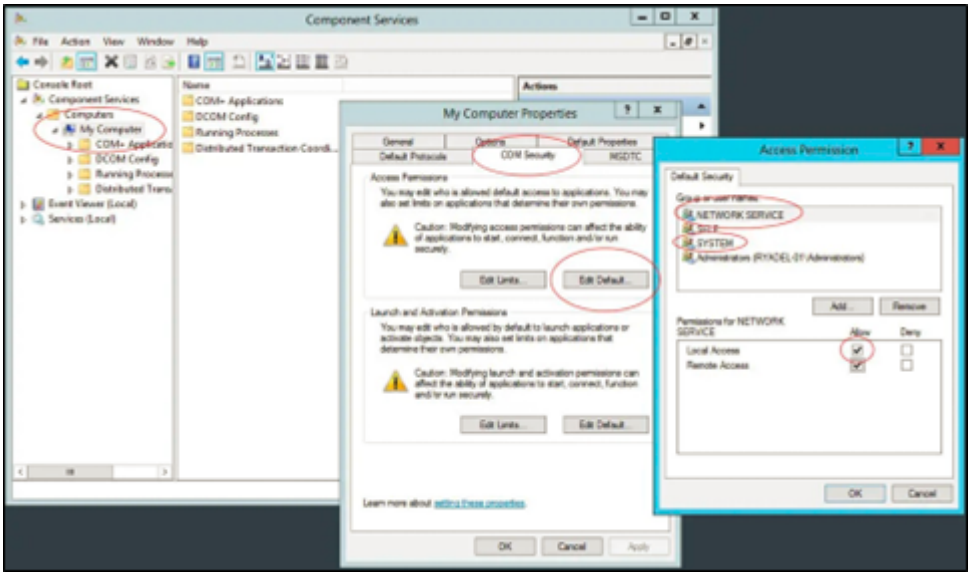


6. Reboot.

Task 3. Validate Component Services Permissions

To validate Component Services permissions, perform the following steps.

1. Open Component Services (Start –> Run –> dcomcnfg).
2. Expand Component Services –> Computers –> My Computer.
3. Right click **My Computer** and select **Properties**.
4. Select the **COM Security** tab.
5. At the Access Permissions option panel select **Edit Default**.
6. Add SYSTEM, NETWORK SERVICE users, and grant Local Access, as shown below.



7. Reboot.

Task 4. Modify MSLLDP Driver's Security Permissions

During backup, a VSS process running under NETWORK_SERVICE account calls cryptcatsvc!CSystemWriter::AddLegacyDriverFiles(), which enumerates all the driver's records in the Service Control Manager database and tries to open each one of them.

Because MSLLDP driver's security permissions do not allow NETWORK_SERVICE to access the driver record, the function fails on MSLLDP record with an "Access Denied" error.

The original security descriptor is displayed 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 is displayed below:

>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.

Adding Access Rights for NT AUTHORITY\SERVICE to MSLLDP Service

To add access rights for NT AUTHORITY\SERVICE to MSLLDP service, perform the following steps.

Important: Use your security descriptor for MSLLDP driver since there can be some cases where it is different for your machine.

Do not copy the SDDL description in this article.

1. Run: SC sdshow MSLLDP.
   The following result is displayed (SDDL language is in Microsoft's documentation):
   > SC sdshow 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)S:(AU;
FA;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;WD)

2. Run: SC sdshow MUP.
   The following result is displayed:

   >SC sdshow MUP
   D:(A;;CCLCSWRPWPDTLOCRRC;;;SY)(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)(A;;CCLCSWL
   OCRRC;;;IU)(A;;CCLCSWLOCRRC;;;SU)S:(AU;FA;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;WD)

3. Copy the 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, as shown below.

   >sc sdset MSLLDP
   D:(D;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BG)(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;SY)
   (A;;CCDCLCSWRPDTLOCRSDRCWDWO;;;BA)(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;SO)(A;;L
   CRPWP;;;S-1-5-80-3141615172-2057878085-1754447212-2405740020-3916490453)(A;;CCLCS
   WLOCRRC;;;SU)S:(AU;FA;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;WD)

5. Check the following 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

6. Run the backup.

Figures