# VMware Snapshot Quiesce Fails due to VMware Snapshot Provider Issue

https://campus.barracuda.com/doc/96015967/

This page provides the following content:



## Issue

VMware Snapshot application quiesce fails due to guest OS VSS Problems.

> There are many possible causes for quiesce failures. This article describes a specific  situation, based on the observed behavior.

## Resolution

This section includes the following topics:



#### Confirm Issue

If VMware backups fail at the snapshot creation step (should be failed 3 times) and the following error message displays in the action logs:

"{VMName} application quiesce failed", perform the following steps.

1. Open up the event viewer of the Guest OS of the backed up VM.
   **Note**: If the VM is powered off, this problem does not occur.
2. Confirm the problem using the following criteria:

- In the "System" event viewer section the following message is displayed:

"Source: Service Control Manager Event ID: 7034

Details:

The VMware Snapshot Provider service terminated unexpectedly. It has done this {N} time(s)."

where N can vary depending on how many times this failed in a row.

- In the "Application" event viewer section the following message is displayed:

"Source: VMware tools

Event ID: 1000

Details:

2021-08-31T15:22:53.590Z] [ error] [vmvss] ASSERT d:/build/ob/bora-18114299/bora-vmsoft/apps/vmtoolslib/vmtoolsConfig.c:572"

**Notes**:

- The internal assert stack trace may differ depending on which version of VMware Tools is currently installed. As a best practice, ensure that the latest version of VMware tools is installed.
- This is a VSS bug currently that is tracked by the user community, for which there is a workaround.
- The community is tracking this problem on this page https://communities.vmware.com/t5/VMware-vSphere-Discussions/Problem-with-Windows-Server-2019-snapshot-quiescing/td-p/2221408
- It has been confirmed to be affecting multiple Windows Server OSs, which go beyond the OS reported in the forum.

#### Workaround

The workaround for this issue is to disable the VMware Snapshot Provider service in the VM's guest OS.

To work around this issue, perform the following steps.

1. Logon to the guest OS for the VM.
2. Select **Start** -> **Run**.
3. Open up the Windows services: run "services.msc".
4. Right click **VSS Snapshot Provider** and select **Properties**.
5. In Startup type dropdown menu, select **Disabled**.

6. Click **Apply** and then close the management console.
7. Restart the guest OS.
8. Rerun the backup.

## Secondary Issue

The following issue is not necessary to fix the quiescing problem, however, sometimes this error accompanies the first one, therefore it is documented here to eliminate all error conditions involved in this scenario.

Sometimes the first error is accompanied by event id 513 in the "Application" event viewer log reported for "CAPI2" source with following description:

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

Details:

AddLegacyDriverFiles: Unable to back up image of binary Microsoft Link-Layer Discovery Protocol.

System Error:

Access is denied."

To fix the problem, see https://docs.microsoft.com/en-US/troubleshoot/windows-server/backup-and-storage/event-id-513-vss-windows-server, also see below.

## Secondary Resolution

Although listed here for completeness, it is not necessary to fix the secondary issue to repair application level quiescing.

To work around the secondary issue, perform the following steps.

1. Open an administrative Command Prompt window, and then run the following command to check the current permissions:
   sc sdshow mslldp
2. Copy the output string from step 1, append it with (A;;CCLCSWLOCRRC;;;SU), and then run the following command to add the access permission to Mslldp.dll:

sc sdset mslldp <string>

3. Restart the computer.

**Note**: Restart may be necessary in certain systems. An administrator may skip this step. if the problem is still manifest, reboot the guest OS.

## References

For more information related to these errors and warnings, refer to VMware's Knowledge Base: https://kb.vmware.com/s/article/2006849.