



# **Share-based backups with Remote VSS**

**ONTAP 9**

NetApp  
April 18, 2023

# Table of Contents

- Share-based backups with Remote VSS . . . . . 1
  - Share-based backups with Remote VSS overview . . . . . 1
  - Remote VSS concepts . . . . . 1
  - Example of a directory structure used by Remote VSS . . . . . 2
  - How SnapManager for Hyper-V manages Remote VSS-based backups for Hyper-V over SMB . . . . . 3

# Share-based backups with Remote VSS

## Share-based backups with Remote VSS overview

You can use Remote VSS to perform share-based backups of Hyper-V virtual machine files that are stored on a CIFS server.

Microsoft Remote VSS (Volume Shadow Copy Services) is an extension of the existing Microsoft VSS infrastructure. Previously, VSS could be used for backup services only for data stored on local disk. This limited the use of VSS to applications that store data either on a local disk or on SAN-based storage. With Remote VSS, Microsoft has extended the VSS infrastructure to support the shadow copying of SMB shares. Server applications such as Hyper-V are now storing VHD files on SMB file shares. With these new extensions, it is possible to take application consistent shadow copies for virtual machines that store data and configuration files on shares.

## Remote VSS concepts

You should be aware of certain concepts that are required to understand how Remote VSS (Volume Shadow Copy Service) is used by backup services with Hyper-V over SMB configurations.

- **VSS (Volume Shadow Copy Service)**

A Microsoft technology that is used to take backup copies or snapshots of data on a specific volume at a specific point in time. VSS coordinates among data servers, backup applications, and storage management software to support the creation and management of consistent backups.

- **Remote VSS (Remote Volume Shadow Copy Service)**

A Microsoft technology that is used to take share-based backup copies of data that is in a data-consistent state at a specific point in time where the data is accessed over SMB 3.0 shares. Also known as *Volume Shadow Copy Service*.

- **Shadow copy**

A duplicate set of data contained in the share at a well-defined instant in time. Shadow copies are used to create consistent point-in-time backups of data, allowing the system or applications to continue updating data on the original volumes.

- **Shadow copy set**

A collection of one or more shadow copies, with each shadow copy corresponding to one share. The shadow copies within a shadow copy set represent all the shares that must be backed up in the same operation. The VSS client on the VSS-enabled application identifies which shadow copies to include in the set.

- **Shadow copy set automatic recovery**

The part of the backup process for remote VSS-enabled backup applications where the replica directory containing the shadow copies is made point-in-time consistent. At the start of the backup, the VSS client on the application triggers the application to take software checkpoints on the data scheduled for backup (the virtual machine files in the case of Hyper-V). The VSS client then allows the applications to continue. After

the shadow copy set is created, Remote VSS makes the shadow copy set writeable and exposes the writeable copy to the applications. The application prepares the shadow copy set for backup by performing an automatic recovery using the software checkpoint taken earlier. Automatic recovery brings the shadow copies into a consistent state by unrolling the changes made to the files and directories since the checkpoint was created. Automatic recovery is an optional step for VSS-enabled backups.

- **Shadow copy ID**

A GUID that uniquely identifies a shadow copy.

- **Shadow copy set ID**

A GUID that uniquely identifies a collection of shadow copy IDs to the same server.

- **SnapManager for Hyper-V**

The software that automates and simplifies backup-and-restore operations for Microsoft Windows Server 2012 Hyper-V. SnapManager for Hyper-V uses Remote VSS with automatic recovery to back up Hyper-V files over SMB shares.

#### **Related information**

[Key concepts about nondisruptive operations for Hyper-V and SQL Server over SMB](#)

[Share-based backups with Remote VSS](#)

## **Example of a directory structure used by Remote VSS**

Remote VSS traverses the directory structure that stores Hyper-V virtual machine files as it creates shadow copies. It is important to understand what an appropriate directory structure is, so that you can successfully create backups of virtual machine files.

A supported directory structure for the successful creation of shadow copies conforms to the following requirements:

- Only directories and regular files are present within the directory structure that is used to store virtual machine files.

The directory structure does not contain junctions, links, or non-regular files.

- All files for a virtual machine reside within a single share.
- The directory structure that is used to store virtual machine files does not exceed the configured depth of the shadow copy directory.
- The root directory of the share contains only virtual machine files or directories.

In the following illustration, the volume named `vm_vol1` is created with a junction point at `/hyperv/vm1` on storage virtual machine (SVM) `vs1`. Subdirectories to contain the virtual machine files are created under the junction point. The virtual machine files of the Hyper-V server are accessed over `share1` that has the path `/hyperv/vm1/dir1/vmdir`. The shadow copy service creates shadow copies of all the virtual machine files that are contained within the directory structure under `share1` (up to the configured depth of the shadow copy directory).



## How SnapManager for Hyper-V manages Remote VSS-based backups for Hyper-V over SMB

You can use SnapManager for Hyper-V to manage Remote VSS-based backup services. There are benefits to using SnapManager for Hyper-V managed backup service to create space efficient backup sets.

Optimizations to SnapManager for Hyper-V managed backups include the following:

- SnapDrive integration with ONTAP provides performance optimization when discovering SMB share location.

ONTAP provides SnapDrive with the name of the volume where the share resides.

- SnapManager for Hyper-V specifies the list of virtual machine files in the SMB shares that the shadow copy service needs to copy.

By providing a targeted list of virtual machine files, the shadow copy service does not need to create shadow copies of all the files in the share.

- The storage virtual machine (SVM) retains the Snapshot copies for SnapManager for Hyper-V to use for restores.

There is no backup phase. The backup is the space-efficient Snapshot copy.

SnapManager for Hyper-V provides backup and restore capabilities for HyperV over SMB using the following process:

## 1. Preparing for the shadow copy operation

The SnapManager for Hyper-V application's VSS client sets up the shadow copy set. The VSS client gathers information about what shares to include in the shadow copy set and provides this information to ONTAP. A set might contain one or more shadow copies, and one shadow copy corresponds to one share.

## 2. Creating the shadow copy set (if automatic-recovery is used)

For every share included in the shadow copy set, ONTAP creates a shadow copy and makes the shadow copy writable.

## 3. Exposing the shadow copy set

After ONTAP creates the shadow copies, they are exposed to SnapManager for Hyper-V so that the application's VSS writers can perform automatic recovery.

## 4. Automatically recovering the shadow copy set

During the shadow copy set creation, there is a period of time when active changes are occurring to the files included in the backup set. The application's VSS writers must update the shadow copies to make sure that they are in a completely consistent state prior to backup.



The way that automatic recovery is done is application specific. Remote VSS is not involved in this phase.

## 5. Completing and cleaning up the shadow copy set

The VSS client notifies ONTAP after it completes automatic recovery. The shadow copy set is made read-only and then is ready for backup. When using SnapManager for Hyper-V for backup, the files in a Snapshot copy become the backup; therefore, for the backup phase, a Snapshot copy is created for every volume containing shares in the backup set. After the backup is complete, the shadow copy set is removed from the CIFS server.

## Copyright information

Copyright © 2023 NetApp, Inc. All Rights Reserved. Printed in the U.S. No part of this document covered by copyright may be reproduced in any form or by any means—graphic, electronic, or mechanical, including photocopying, recording, taping, or storage in an electronic retrieval system—without prior written permission of the copyright owner.

Software derived from copyrighted NetApp material is subject to the following license and disclaimer:

THIS SOFTWARE IS PROVIDED BY NETAPP “AS IS” AND WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, WHICH ARE HEREBY DISCLAIMED. IN NO EVENT SHALL NETAPP BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

NetApp reserves the right to change any products described herein at any time, and without notice. NetApp assumes no responsibility or liability arising from the use of products described herein, except as expressly agreed to in writing by NetApp. The use or purchase of this product does not convey a license under any patent rights, trademark rights, or any other intellectual property rights of NetApp.

The product described in this manual may be protected by one or more U.S. patents, foreign patents, or pending applications.

LIMITED RIGHTS LEGEND: Use, duplication, or disclosure by the government is subject to restrictions as set forth in subparagraph (b)(3) of the Rights in Technical Data -Noncommercial Items at DFARS 252.227-7013 (FEB 2014) and FAR 52.227-19 (DEC 2007).

Data contained herein pertains to a commercial product and/or commercial service (as defined in FAR 2.101) and is proprietary to NetApp, Inc. All NetApp technical data and computer software provided under this Agreement is commercial in nature and developed solely at private expense. The U.S. Government has a non-exclusive, non-transferrable, nonsublicensable, worldwide, limited irrevocable license to use the Data only in connection with and in support of the U.S. Government contract under which the Data was delivered. Except as provided herein, the Data may not be used, disclosed, reproduced, modified, performed, or displayed without the prior written approval of NetApp, Inc. United States Government license rights for the Department of Defense are limited to those rights identified in DFARS clause 252.227-7015(b) (FEB 2014).

## Trademark information

NETAPP, the NETAPP logo, and the marks listed at <http://www.netapp.com/TM> are trademarks of NetApp, Inc. Other company and product names may be trademarks of their respective owners.