



Create backup policies for SQL Server databases

SnapCenter Software

Nirupama Sriram, Archana, Soumik Das
June 16, 2021

This PDF was generated from https://docs.netapp.com/us-en/snapcenter/protect-scsql/task_create_backup_policies_for_sql_server_databases.html on June 18, 2021. Always check docs.netapp.com for the latest.

Table of Contents

Create backup policies for SQL Server databases 1

Create backup policies for SQL Server databases

You can create a backup policy for the resource or the resource group before you use SnapCenter to back up SQL Server resources, or you can create a backup policy at the time you create a resource group or backup a single resource.

What you will need

- You must have defined your data protection strategy.
- You must have prepared for data protection by completing tasks such as installing SnapCenter, adding hosts, identifying resources, and creating storage system connections.
- You must have configured the host log directory for log backup.
- You must have refreshed (discovered) the SQL Server resources.
- If you are replicating Snapshot copies to a mirror or vault, the SnapCenter administrator must have assigned the storage virtual machines (SVMs) for both the source volumes and destination volumes to you.

For information about how administrators assign resources to users, see the SnapCenter installation information.

- If you want to run the PowerShell scripts in prescripts and postscripts, you should set the value of the `usePowershellProcessforScripts` parameter to `true` in the `web.config` file.

The default value is `false`



About this task

A backup policy is a set of rules that governs how you manage and retain backups, and how frequently the resource or resource group is backed up. Additionally, you can specify replication and script settings. Specifying options in a policy saves time when you want to reuse the policy for another resource group.

Most of the fields on these wizard pages are self-explanatory. The following information describes some of the fields for which you might require guidance.

Steps

1. In the left navigation pane, click **Settings**.
2. In the Settings page, click **Policies**.
3. Click **New**.
4. On the **Name** page, enter the policy name and description.
5. On the **Backup Type** page, perform the following steps:
 - a. Choose the backup type:

If you want to...	Do this...
Back up the database files and transaction logs and to truncate the transaction logs	i. Select Full backup and Log backup . ii. Enter the maximum number of databases that should be backed up for each Snapshot copy. <div>  <p>You must increase this value if you want to run multiple backup operations concurrently.</p> </div>
Back up the database files	i. Select Full backup . ii. Enter the maximum number of databases that should be backed up for each Snapshot copy. <div>  <p>You must increase this value if you want to run multiple backup operations concurrently.</p> </div>
Back up the transaction logs	Select Log backup .

- b. If you are backing up your resources by using another backup application, select **Copy only backup**.

Keeping the transaction logs intact allows any backup application to restore the databases. You typically should not use the copy only option in any other circumstance.



Microsoft SQL does not support the **Copy only backup** option together with the **Full backup and Log backup** option for secondary storage.

- c. In the Availability Group Settings section, perform the following actions:

For this field...	Do this...
Backup on preferred backup replica only	Select this option to backup only on preferred backup replica. The preferred backup replica is decided by the backup preferences configured for the AG in the SQL Server.
Select replicas for backup	Choose the primary AG replica or the secondary AG replica for the backup.

For this field...	Do this...
Backup priority (Minimum and Maximum backup priority)	Specify a minimum backup priority number, and a maximum backup priority number that decide the AG replica for backup. For example, you can have a minimum priority of 10 and a maximum priority of 50. In this case, all the AG replicas with a priority more than 10 and less than 50 are considered for backup.



In cluster configurations, the backups are retained at each node of the cluster according to the retention settings set in the policy. If the owner node of the AG changes, the backups are taken according to the retention settings and the backups of the previous owner node will be retained. The retention for AG is applicable only at the node level.

- d. If you want to schedule the backup that you want to create with this policy, specify the schedule type by selecting either **On demand**, **Hourly**, **Daily**, **Weekly**, or **Monthly**.

You can select one schedule type for a policy.

Schedule frequency

Select how often you want the schedules to occur in the policy. The specific times are set at backup job creation enabling you to stagger your start times.

- ☒ On demand
☐ Hourly
☐ Daily
☐ Weekly
☐ Monthly



You can specify the schedule (start date, end date, and frequency) for backup operation while creating a resource group. This enables you to create resource groups that share the same policy and backup frequency, but lets you assign different backup schedules to each policy.



If you have scheduled for 2:00 a.m., the schedule will not be triggered during daylight saving time (DST).



6. On the **Retention** page, depending on the backup type selected in the backup type page, perform one or more of the following actions:

- a. In the Retention settings for the up-to-the-minute restore operation section, perform one of the following actions:


If you want to...	Do this...
Retain only a specific number of Snapshot copies	Select the Keep log backups applicable to last <number> full backups option, and specify the number of Snapshot copies to be retained. If you near this limit, you might want to delete older copies.

If you want to...	Do this...
Retain the backup copies for a specific number of days	Select the Keep log backups applicable to last <number> days of full backups option, and specify the number of days to keep the log backup copies.

- b. In the **Full backup retentions settings** section for the On Demand retention settings, perform the following actions:

For this field...	Do this...
Total Snapshot copies to keep	<p>If you want to specify the number of Snapshot copies to keep, select Total Snapshot copies to keep.</p> <p>If the number of Snapshot copies exceeds the specified number, the Snapshot copies are deleted with the oldest copies deleted first.</p> <div>  <p>The maximum retention value is 1018 for resources on ONTAP 9.4 or later, and 254 for resources on ONTAP 9.3 or earlier. Backups will fail if retention is set to a value higher than what the underlying ONTAP version supports.</p> </div> <div>  <p>You must set the retention count to 2 or higher if you plan to enable SnapVault replication. If you set the retention count to 1, the retention operation might fail because the first Snapshot copy is the reference Snapshot copy for the SnapVault relationship until a newer Snapshot copy is replicated to the target.</p> </div>
Keep Snapshot copies for	If you want to specify the number of days for which you want to keep the Snapshot copies before deleting them, select Keep Snapshot copies for .

- c. In the **Full backup retentions settings** section for the Hourly, Daily, Weekly and Monthly retention settings, specify the retention settings for the schedule type selected on **Backup Type** page.

For this field...	Do this...
Total Snapshot copies to keep	<p>If you want to specify the number of Snapshot copies to keep, select Total Snapshot copies to keep. If the number of Snapshot copies exceeds the specified number, the Snapshot copies are deleted with the oldest copies deleted first.</p> <div>  <p>You must set the retention count to 2 or higher if you plan to enable SnapVault replication. If you set the retention count to 1, the retention operation might fail because the first Snapshot copy is the reference Snapshot copy for the SnapVault relationship until a newer Snapshot copy is replicated to the target.</p> </div>
Keep Snapshot copies for	<p>If you want to specify the number of days for which you want to keep the Snapshot copies before deleting them, select Keep Snapshot copies for.</p>

The log Snapshot copy retention is set to 7 days by default. Use Set-SmPolicy cmdlet to change the log Snapshot copy retention.


This example sets the log Snapshot copy retention to 2:

```
Set-SmPolicy -PolicyName 'newpol' -PolicyType 'Backup'
-PluginPolicyType 'SCSQL' -sqlbackuptype 'FullBackupAndLogBackup'
-RetentionSettings
@{BackupType='DATA';ScheduleType='Hourly';RetentionCount=2},{BackupType='LOG_SNAPSHOT';ScheduleType='None';RetentionCount=2},{BackupType='LOG';ScheduleType='Hourly';RetentionCount=2} -schedulescheduletype 'Hourly'
```

SnapCenter retains Snapshot copies of the database

7. On the **Replication** page, specify replication to the secondary storage system:

For this field...	Do this...
Update SnapMirror after creating a local Snapshot copy	Select this option to create mirror copies of backup sets on another volume (SnapMirror).
Update SnapVault after creating a Snapshot copy	Select this option to perform disk-to-disk backup replication.

For this field...	Do this...
Secondary policy label	<p>Select a Snapshot label.</p> <p>Depending on the Snapshot copy label that you select, ONTAP applies the secondary Snapshot copy retention policy that matches the label.</p> <div>  <p>If you have selected Update SnapMirror after creating a local Snapshot copy, you can optionally specify the secondary policy label. However, if you have selected Update SnapVault after creating a local Snapshot copy, you should specify the secondary policy label.</p> </div>
Error retry count	Enter the number of replication attempts that should occur before the process halts.

8. On the **Script** page, enter the path and the arguments of the prescript or postscript that should be run before or after the backup operation, respectively.

For example, you can run a script to update SNMP traps, automate alerts, and send logs.



You must configure the SnapMirror retention policy in ONTAP so that the secondary storage does not reach the maximum limit of Snapshot copies.

9. On the **Verification** page, perform the following steps:
- In the **Run verification for following backup schedules** section, select the schedule frequency.
 - In the **Database consistency check options** section, perform the following actions:

For this field...	Do this...
Limit the integrity structure to physical structure of the database (PHYSICAL_ONLY)	Select Limit the integrity structure to physical structure of the database (PHYSICAL_ONLY) to limit the integrity check to the physical structure of the database and to detect torn pages, checksum failures, and common hardware failures that impact the database.
Supress all information messages (NO_INFOMSGS)	Select Supress all information messages (NO_INFOMSGS) to suppress all informational messages. Selected by default.
Display all reported error messages per object (ALL_ERRORMSGs)	Select Display all reported error messages per object (ALL_ERRORMSGs) to display all the reported errors per object.

For this field...	Do this...
Do not check nonclustered indexes (NOINDEX)	Select Do not check nonclustered indexes (NOINDEX) if you do not want to check nonclustered indexes. The SQL Server database uses Microsoft SQL Server Database Consistency Checker (DBCC) to check the logical and physical integrity of the objects in the database.
Limit the checks and obtain the looks instead of using an internal database Snapshot copy (TABLOCK)	Select Limit the checks and obtain the looks instead of using an internal database Snapshot copy (TABLOCK) to limit the checks and obtain locks instead of using an internal database Snapshot copy.

- c. In the **Log Backup** section, select **Verify log backup upon completion** to verify the log backup upon completion.
 - d. In the **Verification script settings** section, enter the path and the arguments of the prescript or postscript that should be run before or after the verification operation, respectively.
10. Review the summary, and then click **Finish**.

Copyright Information

Copyright © 2021 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.

RESTRICTED RIGHTS LEGEND: Use, duplication, or disclosure by the government is subject to restrictions as set forth in subparagraph (c)(1)(ii) of the Rights in Technical Data and Computer Software clause at DFARS 252.277-7103 (October 1988) and FAR 52-227-19 (June 1987).

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.