



Create backup policies for Exchange Server databases

SnapCenter Software

Soumik Das, Archana
June 16, 2021

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

Table of Contents

Create backup policies for Exchange Server databases 1

Create backup policies for Exchange Server databases

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

What you will need

- You must have defined your data protection strategy.

For details, see the information about defining a data protection strategy for Exchange databases.

- 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 refreshed (discovered) the Exchange 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.
- 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 script settings. Specifying options in a policy saves time when you want to reuse the policy for another resource group.

Full backup retention is specific to a given policy. A database or resource using policy A with a full backup retention of 4 retains 4 full backups and has no effect on policy B for the same database or resource, which might have a retention of 3 to retain 3 full backups.


Log backup retention is effective across policies, and applies to all log backups for a database or resource. Therefore, when a full backup is performed using policy B, the log retention setting affects log backups created by policy A on the same database or resource. Similarly, the log retention setting for policy A affects log backups created by policy B on the same database.

Best Practice: It's best that you configure the secondary retention policy based on the number of full and log backups, overall, that you want to retain. When you configure secondary retention policies, keep in mind that when databases and logs that are in different volumes, each backup can have three Snapshot copies, and when databases and logs are in the same volume, each backup can have two Snapshot copies.

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 backup type:

If you want to...	Do this...
Back up the database files and the required transaction logs	<p>Select Full backup and Log backup.</p> <p>Databases are backed up with log truncation, and all logs are backed up, including the truncated logs.</p> <div>  <p>This is the recommended backup type.</p> </div>
Back up the database files and the uncommitted transaction logs	<p>Select Full backup.</p> <p>Databases are backed up with log truncation, and truncated logs are not backed up.</p>
Back up all the transaction logs	<p>Select Log backup.</p> <p>All transaction logs on the active file system are backed up, and there is no log truncation.</p> <p>A <i>scebackupinfo</i> directory is created on the same disk as the live log. This directory contains the pointer to the incremental changes for the Exchange database and it is not equivalent to the complete log files.</p>
Back up all database files and transaction logs without truncating the transaction log files	<p>Select Copy Backup.</p> <p>All databases and all logs are backed up, and there is no log truncation. You typically use this backup type for reseeding a replica or for testing or diagnosing a problem.</p>



You should define the space required for log backups based on the full backup retention and not based on Up-to-the-minute (UTM) retention.

- b. In the Database Availability Group Settings section, select an action:

For this field...	Do this...
Back up active copies	<p>Select this option to back up only the active copies of the selected database.</p> <p>For database availability groups (DAGs), this option backs up only active copies of all databases in the DAG.</p> <p>Passive copies are not backed up.</p>
Back up copies on servers to be selected at backup job creation time	<p>Select this option to back up any copies of the databases on the selected servers, both active and passive.</p> <p>For DAGs, this option backs up both active and passive copies of all databases on the selected servers.</p>



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 cluster changes, the backups of the previous owner node will be retained. The retention is applicable only at the node level.

- c. In the Schedule frequency section, select one or more of the frequency types: **On demand**, **Hourly**, **Daily**, **Weekly**, and **Monthly**.



You can specify the schedule (start date, end date) for backup operations 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, configure the retention settings.

The options displayed depend upon the backup type and frequency type you previously selected.



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.



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.

- a. In the Log backups retention settings section, select one of the following:

If you want to...	Do this...
Retain only a specific number of log backups	<p>Select Number of full backups for which logs are retained, and specify the number of full backups for which you want up-to-the-minute restorability.</p> <p>Up-to-the-minute (UTM) retention applies to log backup created via full or log backup. For example, if UTM retention settings is configured to retain log backups of the last 5 full backups, then the log backups of the last 5 full backups are retained.</p> <p>The log folders created as part of full and log backups are automatically deleted as part of UTM. You cannot delete the log folders manually. For example, if the retention setting of full or full and log backup is set for 1 month and UTM retention is set to 10 Days, then the log folder created as part of these backups will be deleted as per UTM. As a result, only 10 days log folders will be there and all other backups are marked for point-in-time restore.</p> <p>You can set UTM retention value as 0, if you do not want to perform up-to-the-minute restore. This will enable point-in-time restore operation.</p> <p>Best Practice: It's best that the setting must be equal to the setting for Total Snapshot copies (full backups) in the Full backup retention settings section. This ensures that log files are retained for each full backup.</p>
Retain the backup copies for a specific number of days	<p>Select the Keep log backups for last option, and specify the number of days to keep the log backup copies.</p> <p>The log backups up to the number of days of full backups are retained.</p>

If you selected **Log backup** as the backup type, log backups are retained as part of the up-to-the-minute retention settings for full backups.

- b. In the Full backup retention settings section, select one of the following for on-demand backups, and then select one for full backups:

For this field...	Do this...
Retain only a specific number of Snapshot copies	<p>If you want to specify the number of full backups to keep, select the Total Snapshot copies to keep option, and specify the number of Snapshot copies (full backups) to retain.</p> <p>If the number of full backups exceeds the specified number, the full backups that exceed the specified number are deleted, with the oldest copies deleted first.</p>
Retain full backups for a specific number of days	Select the Keep Snapshot copies for option, and specify the number of days to keep Snapshot copies (full backups).



If you have a database with only log backups and no full backups on a host in a DAG configuration, the log backups are retained in the following ways:


- By default, SnapCenter finds the oldest full backup for this database in all the other hosts in the DAG, and deletes all log backups on this host that were taken before the full backup.
- You can override the above default retention behavior for a database on a host in a DAG with only log backups by adding the key **MaxLogBackupOnlyCountWithoutFullBackup** in the *C:\Program Files\NetApp\SnapCenter WebApp\web.config* file.

```
<add key="MaxLogBackupOnlyCountWithoutFullBackup" value="10">
```

In the example, the value 10 means you keep up to 10 log backups on the host.

7. On the Replication page, select one or both of the following secondary replication options:

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



You should configure SnapMirror retention policy in ONTAP for the secondary storage to avoid reaching the maximum limit of Snapshot copies on the secondary storage.

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.
 - Prescript backup arguments include “\$Database” and “\$ServerInstance”.
 - Postscript backup arguments include “\$Database”, “\$ServerInstance”, “\$BackupName”, “\$LogDirectory”, and “\$LogSnapshot”.

You can run a script to update SNMP traps, automate alerts, send logs, and so on.

9. 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.