



Backing up and verifying your databases

SnapManager for SAP

NetApp
November 04, 2025

This PDF was generated from <https://docs.netapp.com/us-en/snapmanager-sap/unix-installation-7mode/concept-smsap-isg-snapmanager-backup-overview.html> on November 04, 2025. Always check docs.netapp.com for the latest.

Table of Contents

- Backing up and verifying your databases. 1
 - SnapManager backup overview. 1
 - Defining a backup strategy. 1
 - What mode of SnapManager backup do you need? 1
 - What type of SnapManager backup do you need? 1
 - What type of database profile do you need? 2
 - What naming conventions should be used for Snapshot copies? 2
 - How long do you want to retain backup copies on the primary storage system and the secondary storage system? 2
 - Do you want to verify backup copies using the source volume or a destination volume? 3

Backing up and verifying your databases

After installing SnapManager, you can create a basic backup of your database and verify that backup to ensure it does not contain any corrupt files.

SnapManager backup overview

SnapManager uses NetApp Snapshot technology to create backups of databases. You can use the DBVERIFY utility, or you can use SnapManager to verify the integrity of the backups.

SnapManager backs up a database by creating Snapshot copies of the volumes containing data files, control files, and archive log files. Together, these Snapshot copies comprise a backup set that SnapManager can use to restore a database.

Defining a backup strategy

Defining a backup strategy before creating your backups ensures that you have backups to successfully restore your databases. SnapManager provides flexible granular backup schedule to meet your Service Level Agreement (SLA).



For SnapManager best practices, see *TR 3761*.

What mode of SnapManager backup do you need?

SnapManager supports two modes of backups:

Backup mode	Description
Online backup	Creates a backup of the database when the database is in online state. This backup mode is also called a hot backup.
Offline backup	Creates a backup of the database when the database is either in a mounted or shutdown state. This backup mode is also called a cold backup.

What type of SnapManager backup do you need?

SnapManager supports three types of backups:

Backup type	Description
Full backup	Creates a backup of the entire database, which includes all the datafiles, control files, and archive log files.
Partial backup	Creates a backup of selected datafiles, control files, tablespaces, and archive log files

Backup type	Description
Archive log-only backup	Creates a backup of only the archive log files. You must select Backup Archivelogs Separately while creating the profile.

What type of database profile do you need?

SnapManager creates backups based on whether the database profile separates the archive log backups from the data file backups.

Profile type	Description
A single database profile for combined backup of data files and archive logs	<p>Allows you to create:</p> <ul style="list-style-type: none"> • Full backup containing all the data files, archive log files, and control files • Partial backup containing selected data files, tablespaces, archive log files, and control files
Separate database profiles for archive log backups and data file backups	<p>Allows you to create:</p> <ul style="list-style-type: none"> • Combined backup with different labels for data file backup and archive log backup • Data-files-only backup of all the data files along with the control files • Partial data-files-only backup of selected data files or tablespaces along with the control files • Archive-logs-only backup

What naming conventions should be used for Snapshot copies?

Snapshot copies created by backups can follow a custom naming convention. Custom text or built-in variables such as the profile name, the database name, and the database SID provided by SnapManager can be used to create the naming convention. You can create the naming convention while creating the policy.



You must include the smid variable in the naming format. The smid variable creates a unique Snapshot identifier.

The Snapshot copy naming convention can be changed during or after the creation of a profile. The updated pattern applies only to Snapshot copies that have not yet been created; existing Snapshot copies retain the previous pattern.

How long do you want to retain backup copies on the primary storage system and the secondary storage system?

A backup retention policy specifies the number of successful backups to retain. You can specify the retention policy while creating the policy.

You can select hourly, daily, weekly, monthly, or unlimited as the retention class. For each retention class, you

can specify the retention count and retention duration, either together or individually.

- Retention count determines the minimum number of backups of a particular retention class that should be retained.

For example, if backup schedule is *daily* and retention count is *10*, then 10 daily backups are retained.



The maximum number of Snapshot copies that Data ONTAP allows you can retain is 255. After it reaches the maximum limit, by default the creation of new Snapshot copies fail. However, you can configure the rotation policy in Data ONTAP to delete older Snapshot copies.

- Retention duration determines the minimum number of days for which the backup should be retained.

For example, if backup schedule is *daily* and retention duration is *10*, then 10 days of daily backups are retained.

If you set up SnapMirror replication, the retention policy is mirrored on the destination volume.



For long-term retention of backup copies, you should use SnapVault.

Do you want to verify backup copies using the source volume or a destination volume?

If you use SnapMirror or SnapVault, you can verify backup copies using the Snapshot copy on the SnapMirror or SnapVault destination volume rather than the Snapshot copy on the primary storage system. Using a destination volume for verification reduces the load on the primary storage system.

Copyright information

Copyright © 2025 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.