



Creating a profile for your database

SnapManager Oracle

NetApp

February 05, 2021

Table of Contents

Creating a profile for your database 1

Creating a profile for your database

You must create a profile for your database to perform any operation on that database. The profile contains information about the database and can reference only one database; however, a database can be referenced by multiple profiles. A backup that is created using one profile cannot be accessed from a different profile, even if both profiles are associated with the same database.

You must ensure that target database details are included in the `/etc/oratab` file.

These steps show how to create a profile for your database using the SnapManager UI. You can also use the CLI if you prefer.

For information about how to create profiles using the CLI, see the *SnapManager for Oracle Administration Guide for UNIX*.

1. From the Repositories tree, right-click the repository or the host and select **Create Profile**.
2. On the Profile Configuration Information page, enter the custom name and password for the profile.
3. On the Database Configuration Information page, enter the following information:

In this field...	Do this...
Database Name	Enter the name of the database you want to backup.
Database SID	Enter the secure ID (SID) of the database. The database name and the database SID can be the same.
Host	Enter the IP address of the host where the target database resides. You can also specify the host name if the host name is specified in the Domain Name System (DNS).
Host Account	Enter the Oracle user name of the target database. The default value for the user is oracle.
Host Group	Enter the Oracle user group name. The default value is dba. +

4. On the Database Connection Information page, select one of the following:

Choose this...	If you want to...
Use O/S Authentication	Use the credentials maintained by the operating system to authenticate users who access the database.

Choose this...	If you want to...
Use Database Authentication	<p>Allow Oracle to authenticate an administrative user using password file authentication. Enter the appropriate database connection information.</p> <ul style="list-style-type: none"> • In the SYSDBA Privileged User Name field, enter the name of the database administrator with administrative privileges. • In the Password field, enter the password of the database administrator. • In the Port field, enter the port number used to connect to the host where the database resides. <p>The default value is .</p>
Use ASM Instance Authentication	<p>Allow Automatic Storage Management (ASM) database instance to authenticate an administrative user. Enter the appropriate ASM instance authentication information.</p> <ul style="list-style-type: none"> • In the SYSDBA/SYSASM Privileged User Name field, enter the user name of the ASM instance administrator with administrative privileges. • In the Password field, enter password of the administrator.

Note: You can select the ASM authentication mode only if you have an ASM instance on the database host.

5. On the RMAN Configuration Information page, select one of the following:

Choose this...	If...
Do not use RMAN	You are not using RMAN to manage backup and restore operations.
Use RMAN via the control file	You are managing the RMAN repository using control files.
Use RMAN via Recovery Catalog	<p>You are managing the RMAN repository using recovery catalog database. Enter the user name who has access to recovery catalog database, password, and the Oracle net service name of the database that manages the Transparent Network Substrate (TNS) connection.</p> <p>+</p>

6. On the Snapshot Naming Information page, select the variables to specify a naming format for the Snapshot copy.

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

7. On the Policy Settings page, perform the following:
 - a. Enter the retention count and duration for each retention class.
 - b. From the **Protection Policy** drop-down list, select the Protection Manager policy.
 - c. If you want to back up archive logs separately, select the **Backup Archivelogs Separately** checkbox, specify the retention, and select the protection policy.

You can select a policy which is different from the policy associated for datafiles. For example, if you have selected one of the Protection Manager policy for datafiles, you can select a different Protection Manager policy for archive logs.

8. On the Configure Notification Settings page, specify the email notification settings.
9. On the History Configuration Information page, select one of the options to maintain the history of SnapManager operations.
10. On the Perform Profile Create Operation page, verify the information and click **Create**.
11. Click **Finish** to close the wizard.

If the operation fails, click **Operation Details** to view what caused the operation to fail.

Related information

[SnapManager 3.4 for Oracle Administration Guide for UNIX](#)

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.