



# **Configuring and enabling policy-driven data protection**

## **SnapManager for SAP**

NetApp  
February 12, 2024

This PDF was generated from <https://docs.netapp.com/us-en/snapmanager-sap/unix-administration/task-configure-snapdrive-when-rbac-is-enabled.html> on February 12, 2024. Always check docs.netapp.com for the latest.

# Table of Contents

- Configuring and enabling policy-driven data protection . . . . . 1
  - Configure DataFabric Manager server and SnapDrive when RBAC is enabled . . . . . 1
  - Configure SnapDrive when RBAC is not enabled . . . . . 3
  - Understanding enabling or disabling of data protection in profile . . . . . 3

# Configuring and enabling policy-driven data protection

You must configure SnapDrive and the DataFabric Manager server to enable data protection on the profile to protect backups on the secondary storage systems. You can select the protection policies in the Protection Manager's console to specify how database backups will be protected.



You must ensure that OnCommand Unified Manager is installed on a separate server to enable data protection.

## Configure DataFabric Manager server and SnapDrive when RBAC is enabled

When role-based access control (RBAC) is enabled, you must configure the DataFabric Manager server to include the RBAC capabilities. You must also register the SnapDrive user created in the DataFabric Manager server and root user of the storage system in SnapDrive.

### Steps

1. Configure the DataFabric Manager server.
  - a. To refresh the DataFabric Manager server to update the changes made directly on the storage system by the target database, enter the following command:

```
dfm host discover storage_system
```

- b. Create a new user in the DataFabric Manager server and set the password.
  - c. To add the operating system user to the DataFabric Manager server administration list, enter the following command:

```
dfm user add sd-admin
```

- d. To create a new role in the DataFabric Manager server, enter the following command:

```
dfm role create sd-admin-role
```

- e. To add the DFM.Core.AccessCheck Global capability to the role, enter the following command:

```
dfm role add sd-admin-role DFM.Core.AccessCheck Global
```

- f. To add sd-admin-role to the operating system user, enter the following command:

```
dfm user role set sd-adminsd-admin-role
```

- g. To create another role in the DataFabric Manager server for the SnapDrive root user, enter the following command:

```
dfm role create sd-protect
```

- h. To add RBAC capabilities to the role created for the SnapDrive root user or the administrator, enter the following commands:

```
dfm role add sd-protect SD.Config.Read Global
```

```
dfm role add sd-protect SD.Config.Write Global
```

```
dfm role add sd-protect SD.Config.Delete Global
```

```
dfm role add sd-protect SD.Storage.Read Global
```

```
dfm role add sd-protect DFM.Database.Write Global
```

```
dfm role add sd-protect GlobalDataProtection
```

- i. To add the target database oracle user to the list of administrators in the DataFabric Manager server and assign the sd-protect role, enter the following command:

```
dfm user add -r sd-protecttardb_host1\oracle
```

- j. To add the storage system used by the target database in the DataFabric Manager server, enter the following command:

```
dfm host set storage_system hostLogin=oracle hostPassword=password
```

- k. To create a new role in the storage system used by the target database in the DataFabric Manager server, enter the following command:

```
dfm host role create -h storage_system-c "api-,login-" storage-rbac-role
```

- l. To create a new group in the storage system and assign the new role created in the DataFabric Manager server, enter the following command:

```
dfm host usergroup create -h storage_system-r storage-rbac-rolestorage-rbac-group
```

- m. To create a new user in the storage system and assign the new role and the group created in the DataFabric Manager server, enter the following command:

```
dfm host user create -h storage_system-r storage-rbac-role -p password -g storage-rbac-grouptardb_host1
```

## 2. Configure SnapDrive.

- a. To register the credentials of the *sd-admin* user with SnapDrive, enter the following command:

```
snapdrive config set -dfm sd-admin dfm_host
```

- b. To register the root user or the administrator of the storage system with SnapDrive, enter the following command:

```
snapdrive config set tardb_host1storage_system
```

# Configure SnapDrive when RBAC is not enabled

You must register the root user or the administrator of the DataFabric Manager server and root user of the storage system with SnapDrive to enable data protection.

## Steps

1. To refresh the DataFabric Manager server to update the changes made directly on the storage system by the target database, enter the following command:

### Example

```
dfm host discover storage_system
```

2. To register the root user or the administrator of the DataFabric Manager server with SnapDrive, enter the following command:

### Example

```
snapdrive config set -dfm Administrator dfm_host
```

3. To Register the root user or the administrator of the storage system with SnapDrive, enter the following command:

### Example


```
snapdrive config set root storage_system
```

## Understanding enabling or disabling of data protection in profile

You can enable or disable data protection while creating or updating a database profile.

To create a protected backup of a database on the secondary storage resources, database administrators and storage administrators perform the following actions.

If you want to...	Then...
Create or edit a profile	<p>To create or edit a profile, perform the following:</p> <ul style="list-style-type: none"> <li>• Enable backup protection to the secondary storage.</li> <li>• If you are using Data ONTAP operating in 7-Mode and have installed Protection Manager, you can select the policies created by the storage or backup administrator in Protection Manager.</li> </ul> <p>If you are using Data ONTAP operating in 7-Mode and protection is enabled, SnapManager creates a dataset for the database. A dataset consists of a collection of storage sets along with configuration information associated with their data. The storage sets associated with a dataset include a primary storage set used to export data to clients, and the set of replicas and archives that exist on other storage sets. Datasets represent exportable user data. If the administrator disables protection for a database, SnapManager deletes the dataset.</p> <ul style="list-style-type: none"> <li>• If you are using ONTAP, you must select either the <i>SnapManager_cDOT_Mirror</i> or <i>SnapManager_cDOT_Vault</i> policy depending on the SnapMirror or SnapVault relationship created.</li> </ul> <p>When you disable backup protection, a warning message is displayed stating that the dataset will be deleted and restoring or cloning backups for this profile will not be possible.</p>
View the profile	<p>Because the storage administrator has not yet assigned storage resources to implement the protection policy, the profile shows up as nonconformant in both the SnapManager graphical user interface and the <code>profile show</code> command output.</p>
Assign storage resources in the Protection Manager Management Console	<p>In the Protection Manager Management Console, the storage administrator views the unprotected dataset and assigns a resource pool for each node of the dataset that is associated with the profile. The storage administrator then makes sure that secondary volumes are provisioned and protection relationships are initialized.</p>
View the conformant profile in SnapManager	<p>In SnapManager, the database administrator sees that the profile has changed to conformant state in both the graphical user interface and in the <code>profile show</code> command output, indicating that resources were assigned.</p>

If you want to...	Then...
Create the backup	<ul style="list-style-type: none"> <li>• Select full backup.</li> <li>• Also, select whether the backup should be protected and select the primary retention class (for example, hourly or daily).</li> <li>• If you are using Data ONTAP operating in 7-Mode and want to protect the backup immediately to secondary storage overriding the Protection Manager protection schedule, specify the <code>-protectnow</code> option.</li> <li>• If you are using ONTAP and want to protect the backup immediately to the secondary storage, specify the <code>protect</code> option.</li> </ul> <div data-bbox="669 569 724 625">  </div> <div data-bbox="786 564 1453 630"> <p>The <code>protectnow</code> option is not applicable in clustered Data ONTAP.</p> </div>
View the backup	<p>The new backup is shown as scheduled for protection, but not yet protected (in the SnapManager interface and in the <code>backup show</code> command output). The Protection state is shown as “Not protected”.</p>
View the backup list	<p>After the storage administrator verifies that the backup has been copied to secondary storage, SnapManager changes the backup Protection state from “Not protected” to “Protected”.</p>

## Copyright information

Copyright © 2024 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.