Setting up protection relationships in Unified Manager

OnCommand Unified Manager 9.5

NetApp
February 12, 2024

This PDF was generated from https://docs.netapp.com/us-en/oncommand-unified-manager-95/health-checker/task-configuring-a-connection-between-workflow-automation-and-unified-manager.html on February 12, 2024. Always check docs.netapp.com for the latest.

Table of Contents

Setting up protection relationships in Unified Manager . . . 1
- Before you begin . . . 1
- Steps . . . 1
- Configuring a connection between Workflow Automation and Unified Manager . . . 1
- Verifying Unified Manager data source caching in Workflow Automation . . . 2
- Creating a SnapMirror protection relationship from the Health/Volume details page . . . 3
- Creating a SnapVault protection relationship from the Health/Volume details page . . . 4
- Creating a SnapVault policy to maximize transfer efficiency . . . 5
- Creating a SnapMirror policy to maximize transfer efficiency . . . 5
- Creating SnapMirror and SnapVault schedules . . . 6

Setting up protection relationships in Unified Manager

There are several steps that you must perform to use Unified Manager and OnCommand Workflow Automation to set up SnapMirror and SnapVault relationships to protect your data.

Before you begin

- You must have the OnCommand Administrator or Storage Administrator role.
- You must have established peer relationships between two clusters or two storage virtual machines (SVMs).
- OnCommand Workflow Automation must be integrated with Unified Manager:
  - Set up OnCommand Workflow Automation
  - Verifying Unified Manager data source caching in Workflow Automation

Steps

1. Depending on the type of protection relationship you want to create, do one of the following:
   - Create a SnapMirror protection relationship.
   - Create a SnapVault protection relationship.
2. If you want to create a policy for the relationship, depending on the relationship type you are creating, do one of the following:
   - Create a SnapVault policy.
   - Create a SnapMirror policy.
3. Create a SnapMirror or SnapVault schedule.

Configuring a connection between Workflow Automation and Unified Manager

You can configure a secure connection between OnCommand Workflow Automation (WFA) and Unified Manager. Connecting to Workflow Automation enables you to use protection features such as SnapMirror and SnapVault configuration workflows, as well as commands for managing SnapMirror relationships.

Before you begin

- The installed version of Workflow Automation must be 4.2 or greater.
- You must have installed “WFA pack for managing Clustered Data ONTAP” version 9.5.0 or greater on the WFA server. You can download the required pack from the NetAppStorage Automation Store.

  WFA pack for managing ONTAP

- You must have the name of the database user that you created in Unified Manager to support WFA and Unified Manager connections.

  This database user must have been assigned the Integration Schema user role.

- You must be assigned either the Administrator role or the Architect role in Workflow Automation.
- You must have the host address, port number 443, user name, and password for the Workflow Automation setup.
- You must have the OnCommand Administrator or Storage Administrator role.

Steps

1. In the toolbar, click , and then click **Workflow Automation** in the left Setup menu.
2. In the **OnCommand Unified Manager Database User** area of the **Setup/Workflow Automation** page, select the name, and enter the password for the database user that you created to support Unified Manager and Workflow Automation connections.
3. In the **OnCommand Workflow Automation Credentials** area of the **Setup/Workflow Automation** page, enter the host name or IP address (IPv4 or IPv6), and the user name and password for the Workflow Automation setup.

   You must use theUnified Manager server port (port 443).

4. Click **Save**.
5. If you use a self-signed certificate, click **Yes** to authorize the security certificate.

   The Setup/Workflow Automation page displays.

6. Click **Yes** to reload the web UI, and add the Workflow Automation features.

Verifying Unified Manager data source caching in Workflow Automation

You can determine whether Unified Manager data source caching is working correctly by checking if data source acquisition is successful in Workflow Automation. You might do this when you integrate Workflow Automation with Unified Manager to ensure that Workflow Automation functionality is available after the integration.

Before you begin

You must be assigned either the Administrator role or the Architect role in Workflow Automation to perform this task.

Steps

1. From the Workflow Automation UI, select **Execution** > **Data Sources**.
2. Right-click the name of the Unified Manager data source, and then select **Acquire Now**.
3. Verify that the acquisition succeeds without errors.

   Acquisition errors must be resolved for Workflow Automation integration with Unified Manager to succeed.

Creating a SnapMirror protection relationship from the Health/Volume details page

You can use the Health/Volume details page to create a SnapMirror relationship so that data replication is enabled for protection purposes. SnapMirror replication enables you to restore data from the destination volume in the event of data loss on the source.

Before you begin

- You must have the OnCommand Administrator or Storage Administrator role.
- You must have set up Workflow Automation.

About this task

The **Protect** menu does not display in the following instances:

- If RBAC settings do not allow this action: for example, if you have only operator privileges
- If the volume is a FlexGroup volume
- When the volume ID is unknown: for example, when you have an intercluster relationship and the destination cluster has not yet been discovered

You can perform up to 10 protection jobs simultaneously with no performance impact. You might experience some performance impact when you run between 11 and 30 jobs simultaneously. Running more than 30 jobs simultaneously is not recommended.

Steps

1. In the **Protection** tab of the **Health/Volume** details page, right-click in the topology view the name of a volume that you want to protect.
2. Select **Protect** > **SnapMirror** from the menu.

   The Configure Protection dialog box is displayed.
3. Click **SnapMirror** to view the **SnapMirror** tab and to configure the destination information.
4. Click **Advanced** to set the space guarantee, as needed, and then click **Apply**.
5. Complete the **Destination Information** area and the **Relationship Settings** area in the **Configure Protection** dialog box.
6. Click **Apply**.

   You are returned to the Health/Volume details page.
7. Click the protection configuration job link at the top of the **Health/Volume** details page.

   The job's tasks and details are displayed in the Protection/Job details page.
8. In the **Protection/Job** details page, click **Refresh** to update the tasks list and task details associated with the protection configuration job and to determine when the job is complete.
9. When the job tasks are complete, click **Back** on your browser to return to the **Health/Volume** details page.

The new relationship is displayed in the Health/Volume details page topology view.

Results

Depending on the destination SVM you specified during configuration or on the options you enabled in your Advanced settings, the resulting SnapMirror relationship might be one of several possible variations:

- If you specified a destination SVM that runs under the same or a newer version of ONTAP compared to that of the source volume, a block-replication-based SnapMirror relationship is the default result.
- If you specified a destination SVM that runs under the same or a newer version of ONTAP (version 8.3 or higher) compared to that of the source volume, but you enabled version-flexible replication in the Advanced settings, a SnapMirror relationship with version-flexible replication is the result.
- If you specified a destination SVM that runs under an earlier version of ONTAP 8.3, or a version that is higher than that of the source volume and the earlier version supports version-flexible replication, a SnapMirror relationship with version-flexible replication is the automatic result.

Creating a SnapVault protection relationship from the Health/Volume details page

You can create a SnapVault relationship using the Health/Volume details page so that data backups are enabled for protection purposes on volumes.

Before you begin

- You must have the OnCommand Administrator or Storage Administrator role.
- You must have set up Workflow Automation to perform this task.

About this task

The **Protect** menu does not display in the following instances:

- If RBAC settings do not allow this action: for example, if you have only operator privileges
- When the volume ID is unknown: for example, when you have a intercluster relationship and the destination cluster has not yet been discovered

Steps

1. In the **Protection** tab of the **Health/Volume** details page, right-click a volume in the topology view that you want to protect.
2. Select **Protect** > **SnapVault** from the menu.

   The Configure Protection dialog box is launched.

3. Click **SnapVault** to view the **SnapVault** tab and to configure the secondary resource information.
4. Click **Advanced** to set deduplication, compression, autogrow, and space guarantee as needed, and then click **Apply**.
5. Complete the **Destination Information** area and the **Relationship Settings** area in the **Configure Protection** dialog box.

6. Click **Apply**.

   You are returned to the Health/Volume details page.

7. Click the protection configuration job link at the top of the **Health/Volume** details page.

   The Protection/Job details page is displayed.

8. Click **Refresh** to update the tasks list and task details associated with the protection configuration job and to determine when the job is complete.

   When the job tasks are complete, the new relationships are displayed in the Health/Volume details page topology view.

Creating a SnapVault policy to maximize transfer efficiency

You can create a new SnapVault policy to set the priority for a SnapVault transfer. You use policies to maximize the efficiency of transfers from the primary to the secondary in a protection relationship.

Before you begin

- You must have the OnCommand Administrator or Storage Administrator role.
- You must have set up Workflow Automation.
- You must have already completed Destination Information area in the Configure Protection dialog box.

Steps

1. From the **SnapVault** tab of the **Configure Protection** dialog box, click the **Create Policy** link in the **Relationship Settings** area.

   The SnapVault tab is displayed.

2. In the **Policy Name** field, type the name that you want to give the policy.
3. In the **Transfer Priority** field, select the transfer priority that you want to assign to the policy.
4. In the **Comment** field, enter a comment for the policy.
5. In the **Replication Label** area, add or edit a replication label, as necessary.
6. Click **Create**.

   The new policy is displayed in the Create Policy drop-down list.

Creating a SnapMirror policy to maximize transfer efficiency

You can create a SnapMirror policy to specify the SnapMirror transfer priority for protection relationships. SnapMirror policies enable you to maximize transfer efficiency from the source to the destination by assigning priorities so that lower-priority transfers are scheduled to run after normal-priority transfers.

Before you begin

- You must have the OnCommand Administrator or Storage Administrator role.
- You must have set up Workflow Automation.
- This task assumes that you have already completed the Destination Information area in the Configure Protection dialog box.

Steps

1. From the **SnapMirror** tab of the **Configure Protection** dialog box, click the **Create Policy** link in the **Relationship Settings** area.

   The Create SnapMirror Policy dialog box is displayed.

2. In the **Policy Name** field, type a name you want to give the policy.
3. In the **Transfer Priority** field, select the transfer priority you want to assign to the policy.
4. In the **Comment** field, enter an optional comment for the policy.
5. Click **Create**.

   The new policy is displayed in the SnapMirror Policy drop-down list.

Creating SnapMirror and SnapVault schedules

You can create basic or advanced SnapMirror and SnapVault schedules to enable automatic data protection transfers on a source or primary volume so that transfers take place more frequently or less frequently, depending on how often the data changes on your volumes.

Before you begin

- You must have the OnCommand Administrator or Storage Administrator role..
- You must have already completed the Destination Information area in the Configure Protection dialog box.
- You must have set up Workflow Automation to perform this task.

Steps

1. From the **SnapMirror** tab or **SnapVault** tab of the **Configure Protection** dialog box, click the **Create Schedule** link in the **Relationship Settings** area.

   The Create Schedule dialog box is displayed.

2. In the **Schedule Name** field, type the name you want to give to the schedule.
3. Select one of the following:
   - **Basic**

     Select if you want to create a basic interval-style schedule.

   - **Advanced**

Select if you want to create a cron-style schedule.

4. Click **Create**.

   The new schedule is displayed in the SnapMirror Schedule or SnapVault Schedule drop-down list.

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.