



# **Managing your Infinite Volume with storage classes and data policies**

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-editing-storage-class-threshold-settings.html> on February 12, 2024. Always check docs.netapp.com for the latest.

# Table of Contents

- Managing your Infinite Volume with storage classes and data policies . . . . . 1
  - Before you begin . . . . . 1
  - About this task . . . . . 1
  - Steps . . . . . 2
  - Editing the threshold settings of storage classes . . . . . 2
  - Adding alerts . . . . . 3
  - Creating rules . . . . . 5
  - Exporting a data policy configuration . . . . . 6

# Managing your Infinite Volume with storage classes and data policies

You can effectively manage your Infinite Volume by creating the Infinite Volume with the required number of storage classes, configuring thresholds for each storage class, creating rules and a data policy to determine the placement of data written to the Infinite Volume, configuring data protection, and optionally configuring notification alerts.

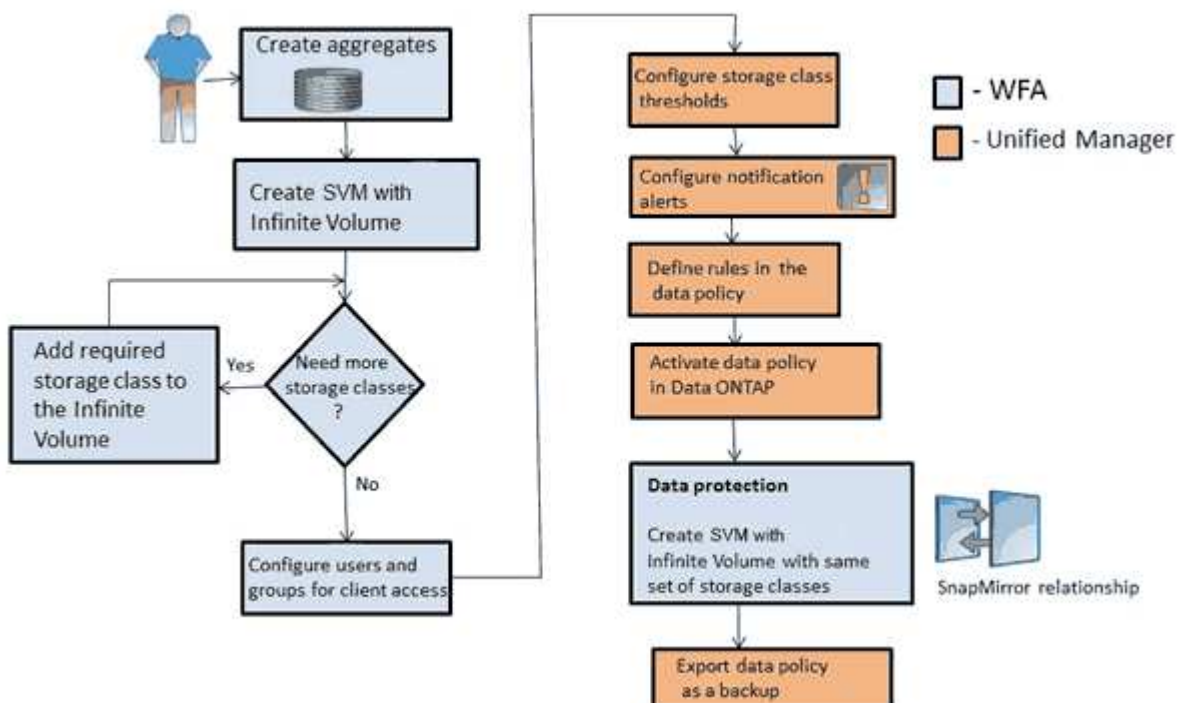
## Before you begin

- OnCommand Workflow Automation (WFA) must be installed.
- You must have the OnCommand Administrator or Storage Administrator role.
- You must have created the required number of aggregates by customizing the appropriate predefined workflow in WFA.
- You must have created the required number of storage classes by customizing the appropriate predefined workflow in WFA.
- You must have configured the Unified Manager server as a data source in WFA, and then you must have verified that the data is cached successfully.

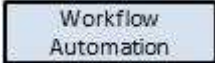
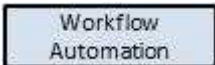

## About this task

While performing this task, you are required to switch between two applications: OnCommand Workflow Automation (WFA) and OnCommand Unified Manager.

The task provides high-level steps. For details about performing the WFA tasks, see the *OnCommand Workflow Automation* documentation.





## Steps

1.  Customize the predefined workflow to define the required storage classes.
2.  Create an SVM with Infinite Volume with the required number of storage classes by using the appropriate workflow.
3.  Add the cluster containing the SVM with Infinite Volume to the Unified Manager database.

You can add the cluster by providing the IP address or the FQDN of the cluster.

4.  [Based on your organization's requirements, modify the thresholds for each storage class.](#)

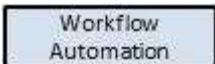
You should use the default storage class threshold settings to effectively monitor storage class space.

5.  [Configure notification alerts and traps to address any availability and capacity issues related to the Infinite Volume.](#)
6.  [Set up rules in the data policy, and then activate all the changes made to the data policy](#)

Rules in a data policy determine the placement of the content written to the Infinite Volume.



Rules in a data policy affect only new data written to the Infinite Volume and do not affect existing data in the Infinite Volume.

7.  Create a disaster recovery (DR) SVM with Infinite Volume, and then configure a data protection (DP) by performing the following steps:
  - a. Create a data protection (DP) Infinite Volume by using the appropriate workflow.
  - b. Set up a DP mirror relationship between the source and destination by using the appropriate workflow.

## Editing the threshold settings of storage classes

When you need to address any issues related to storage space in your storage classes, you can edit the threshold settings of the storage class capacity based on your organization's requirements. When the threshold is crossed, events are generated, and you receive notifications if you have configured alerts for such events.

### Before you begin

You must have the OnCommand Administrator or Storage Administrator role.

## Steps

1. In the left navigation pane, click **Health > SVMs**.
2. In the **Health/Storage Virtual Machines** inventory page, select an SVM with Infinite Volume.
3. In the **Health/Storage Virtual Machine** details page, click **Actions > Edit Thresholds**.
4. In the **Edit Storage Class Thresholds** dialog box, modify the thresholds as required.
5. Click **Save and Close**.

## Adding alerts

You can configure alerts to notify you when a particular event is generated. You can configure alerts for a single resource, for a group of resources, or for events of a particular severity type. You can specify the frequency with which you want to be notified and associate a script to the alert.

### Before you begin

- You must have configured notification settings such as the user email address, SMTP server, and SNMP trap host to enable the Unified Manager server to use these settings to send notifications to users when an event is generated.
- You must know the resources and events for which you want to trigger the alert, and the user names or email addresses of the users that you want to notify.
- If you want to have a script execute based on the event, you must have added the script to Unified Manager by using the Management/Scripts page.
- You must have the OnCommand Administrator or Storage Administrator role.

### About this task

You can create an alert directly from the Event details page after receiving an event in addition to creating an alert from the Configuration/Alerting page, as described here.

## Steps

1. In the left navigation pane, click **Configuration > Alerting**.
2. In the **Configuration/Alerting** page, click **Add**.
3. In the **Add Alert** dialog box, click **Name**, and enter a name and description for the alert.
4. Click **Resources**, and select the resources to be included in or excluded from the alert.

You can set a filter by specifying a text string in the **Name contains** field to select a group of resources. Based on the text string that you specify, the list of available resources displays only those resources that match the filter rule. The text string that you specify is case-sensitive.

If a resource conforms to both the include and exclude rules that you have specified, the exclude rule takes precedence over the include rule, and the alert is not generated for events related to the excluded resource.

5. Click **Events**, and select the events based on the event name or event severity type for which you want to trigger an alert.



To select more than one event, press the Ctrl key while you make your selections.

6. Click **Actions**, and select the users that you want to notify, choose the notification frequency, choose whether an SNMP trap will be sent to the trap receiver, and assign a script to be executed when an alert is generated.



If you modify the email address that is specified for the user and reopen the alert for editing, the Name field appears blank because the modified email address is no longer mapped to the user that was previously selected. Also, if you modified the email address of the selected user from the Management/Users page, the modified email address is not updated for the selected user.

You can also choose to notify users through SNMP traps.

7. Click **Save**.

## Example of adding an alert

This example shows how to create an alert that meets the following requirements:

- Alert name: HealthTest
- Resources: includes all volumes whose name contains “abc” and excludes all volumes whose name contains “xyz”
- Events: includes all critical health events
- Actions: includes “[sample@domain.com](mailto:sample@domain.com)”, a “Test” script, and the user has to be notified every 15 minutes

Perform the following steps in the Add Alert dialog box:

1. Click **Name**, and enter `HealthTest` in the **Alert Name** field.
2. Click **Resources**, and in the Include tab, select **Volumes** from the drop-down list.
  - a. Enter `abc` in the **Name contains** field to display the volumes whose name contains “abc”.
  - b. Select **<<All Volumes whose name contains 'abc'>>** from the Available Resources area, and move it to the Selected Resources area.
  - c. Click **Exclude**, and enter `xyz` in the **Name contains** field, and then click **Add**.
3. Click **Events**, and select **Critical** from the Event Severity field.
4. Select **All Critical Events** from the Matching Events area, and move it to the Selected Events area.
5. Click **Actions**, and enter `sample@domain.com` in the Alert these users field.
6. Select **Remind every 15 minutes** to notify the user every 15 minutes.

You can configure an alert to repeatedly send notifications to the recipients for a specified time. You should determine the time from which the event notification is active for the alert.

7. In the Select Script to Execute menu, select **Test** script .
8. Click **Save**.

# Creating rules

You can add new rules to your data policy to determine the placement of data that is written to the Infinite Volume. You can create rules either by using rule templates that are defined in Unified Manager or create custom rules.

## Before you begin

- You must have the OnCommand Administrator or Storage Administrator role.
- The cluster containing the SVM with Infinite Volume with storage classes must be added to the Unified Manager database.

## Creating rules using templates

You can add new rules by using rule templates defined by Unified Manager to determine the placement of data that is written to the SVM with Infinite Volume. You can create rules based on file types, directory paths, or owners.

## Before you begin

- You must have the OnCommand Administrator or Storage Administrator role.
- The cluster containing the SVM with Infinite Volume with storage classes must be added to the Unified Manager database.

## About this task

The Data Policy tab is visible only for an SVM with Infinite Volume.

## Steps

1. In the left navigation pane, click **Health > SVMs**.
2. In the **Health/Storage Virtual Machines** inventory page, select the appropriate SVM.
3. Click the **Data Policy** tab.

The list of rules in the data policy for the selected SVM with Infinite Volume is displayed.

4. Click **Create**.
5. In the **Create Rule** dialog box, choose an appropriate rule template from the drop-down list.

The template is based on three categories: file type, owner, or directory path.

6. Based on the template selected, add the necessary conditions in the **Matching Criteria** area.
7. Select an appropriate storage class from the **Place the matching content in Storage Class** drop-down list.
8. Click **Create**.

The new rule you created is displayed in the Data Policy tab.

9. Preview any other changes made to the data policy.

10. Click **Activate** to activate the changes in the rule properties in the SVM.

## Creating custom rules

Based on your data center requirements, you can create custom rules and add them to a data policy to determine the placement of data that is written to the SVM with Infinite Volume. You can create custom rules from the Create Rule dialog box without using any existing template.

### Before you begin

- You must have the OnCommand Administrator or Storage Administrator role.
- The cluster containing the SVM with Infinite Volume with storage classes must be added to the Unified Manager database.

### About this task

The Data Policy tab is visible only for an SVM with Infinite Volume.

### Steps

1. In the left navigation pane, click **Health > SVMs**.
2. In the **Health/Storage Virtual Machines** inventory page, select the appropriate SVM.
3. Click **Data Policy**.
4. Click **Create**.
5. In the **Create Rule** dialog box, select **Custom rule** from the **Template** list.
6. In the **Matching Criteria** area, add conditions as required.

Conditions enable you to create a rule based on file types, directory paths, or owners. A combination of these conditions are the condition sets. For example, you can have a rule: "Place all .mp3 owned by John in bronze storage class."

7. Select an appropriate storage class from the **Place the matching content in Storage Class** drop-down list.
8. Click **Create**.

The newly created rule is displayed in the Data Policy tab.

9. Preview any other changes made to the data policy.
10. Click **Activate** to activate the changes in the rule properties in the SVM.

## Exporting a data policy configuration

You can export a data policy configuration from Unified Manager to a file. For example, after you have taken the required backup, and in the event of a disaster, you can export the data policy configuration from the primary.



## Before you begin

You must have the OnCommand Administrator or Storage Administrator role.

## About this task

The Data Policy tab, which is used while performing this task, is displayed only for SVMs with Infinite Volume.

## Steps

1. In the left navigation pane, click **Health > SVMs**.
2. In the **Health/Storage Virtual Machines** inventory page, select the appropriate SVM.
3. Click **Data Policy**.

The list of rules in the data policy for the selected SVM with Infinite Volume is displayed.

4. Click **Export**.
5. In the browser-specific dialog box, specify the location to which the data policy configuration has to be exported.

## Results

The data policy configuration is exported as a JSON file in the specified location.

## 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.