



Ensuring IO density reports describe only internal data volumes

OnCommand Insight

NetApp
October 24, 2024

This PDF was generated from <https://docs.netapp.com/us-en/oncommand-insight/howto/creating-a-query-to-identify-netapp-root-aggregates.html> on October 24, 2024. Always check docs.netapp.com for the latest.

Table of Contents

- Ensuring IO density reports describe only internal data volumes 1
 - Creating a query to identify NetApp root aggregates in your environment 1
 - Create an annotation for the root volumes returned by your queries. 2
 - Create an annotation rule to automate excluding specific aggregates from your I/O density report 2

Ensuring IO density reports describe only internal data volumes

In NetApp storage systems the root aggregate contains the root volume. The root volume contains special directories and configuration files for managing and controlling the storage system. The management and control operations might result a large amount of activity in the root aggregate. When you query the Insight system for the top 10 internal volumes with the highest IO density, your results might include NetApp root aggregates as members of the top 10.

When monitoring your environment it is more important to determine which internal data volumes are producing high I/O density numbers. In order to accurately identify only the data volumes, you need to isolate the NetApp internal volumes from queries you use to monitor I/O density.

This guide describes how to easily identify the NetApp root aggregates, isolate them from the results of internal volume queries, and create rules that exclude any new NetApp root aggregates as they are added to the system. The following Insight features are used to insure that your I/O density reports are derived from internal data volumes.

- A query is created to identify all of the NetApp root aggregates that are monitored by Insight.
- An annotation is assigned to each of the NetApp root aggregates.
- An annotation rule is created to exclude the NetApp aggregates

Creating a query to identify NetApp root aggregates in your environment

Queries provide search at a granular level, based on user-selected criteria. Using a query allows you to search for Internal volumes in your environment that contain the NetApp root aggregate.

Steps

1. In the OnCommand Insight web UI, create a query to identify NetApp root aggregates in your environment:
Queries > New Query > Select Resource Type
2. Click **Storage Pool**
3. Enter the name for the root aggregate

This example uses “aggr0” for the name. When creating an aggregate, only the following requirements for the name must be followed:

- It must begin with either a letter or an underscore (_).
- It can contain only letters, digits, and underscores.
- It can be 250 characters or less. In most cases the aggregate is name aggr0, aggr_0, or something similar. It might require an iterative process to identify all of the NetApp root aggregates in your environment.

4. Click **Save** and enter a name for the new query.

As mentioned before, this might be an iterative process and require multiple queries to identify all of the NetApp root aggregates.

Create an annotation for the root volumes returned by your queries

Annotations are specialized notes that you assign to your assets, allowing you to filter assets by their annotations. The annotation you create will be used to identify the NetApp root aggregates in your environment and ensure that they are not included in a specific report.

Before you begin

You must have identified all of the root aggregates you want to exclude from the “High I/O Density” report.

Steps

1. Create an annotation to associate all of the NetApp root aggregates you identified with queries: **Manage > Annotations**
2. Click **Add**
 - a. Enter the name for the annotation: **RootAggr**
 - b. Enter a description of the annotation: **Remove root aggregate from "High I/O Density" report**
 - c. Enter the type of annotation: **Boolean**
3. Click **Save**

Create an annotation rule to automate excluding specific aggregates from your I/O density report

As an alternative to manually applying annotations to individual assets, you can automatically apply annotations to multiple assets using annotation rules. Annotation rules are based on queries you create and when run on the system they add new assets to existing sets of assets. When these sets of assets are excluded from a report the new assets are automatically excluded too.

Before you begin

You must have created and saved a query that identifies the NetApp root aggregates you identified in your environment.

Steps

1. Log in to the OnCommand Insight web UI.
2. Click **Manage > Annotation rules**
3. Click **Add**

The Add Rule dialog box displays.

4. Do the following:
 - a. In the Name box, enter a unique name that describes the rule: "RootAggrExclude"
 - b. Click Query and select the Query that Insight should use to apply the annotation rule to:" Aggregate0`"
 - c. Click Annotation and select: "Root agg exclude"
 - d. Click Value and enter True

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.