Managing performance policies

OnCommand Insight

NetApp
October 24, 2024

This PDF was generated from https://docs.netapp.com/us-en/oncommand-insight/config-admin/creating-performance-policies.html on October 24, 2024. Always check docs.netapp.com for the latest.

Table of Contents

Managing performance policies 1
Creating performance policies 1
Performance policy evaluation precedence 3
Editing performance policies 4
Deleting performance policies 5

Managing performance policies

OnCommand Insight enables you to create performance policies to monitor your network for various thresholds and to raise alerts when those thresholds are crossed. Using performance policies, you can detect a violation of a threshold immediately, identify the implication, and analyze the impact and root cause of the problem in a manner that enables rapid and effective correction.

A performance policy enables you to set thresholds on any objects (datastore, disk, hypervisor, internal volume, port, storage, storage node, storage pool, VMDK, virtual machine, and volume) with reported performance counters (for example, total IOPS). When a violation of a threshold occurs, Insight detects and reports it in the associated asset page, by displaying a red solid circle; by email alert, if configured; and in the Violations Dashboard or any custom dashboard that reports violations.

Insight provides some default performance policies, which you can modify or delete if they are not applicable to your environment, for the following objects:

- Hypervisor

  There are ESX swapping and ESX utilization policies.

- Internal volume and volume

  There are two latency policies for each resource, one annotated for Tier 1 and the other annotated for Tier 2.

- Port

  There is a policy for BB credit zero.

- Storage node

  There is a policy for node utilization.

- Virtual machine

  There are VM swapping and ESX CPU and memory policies.

- Volume

  There are latency by tier and misaligned volume policies.

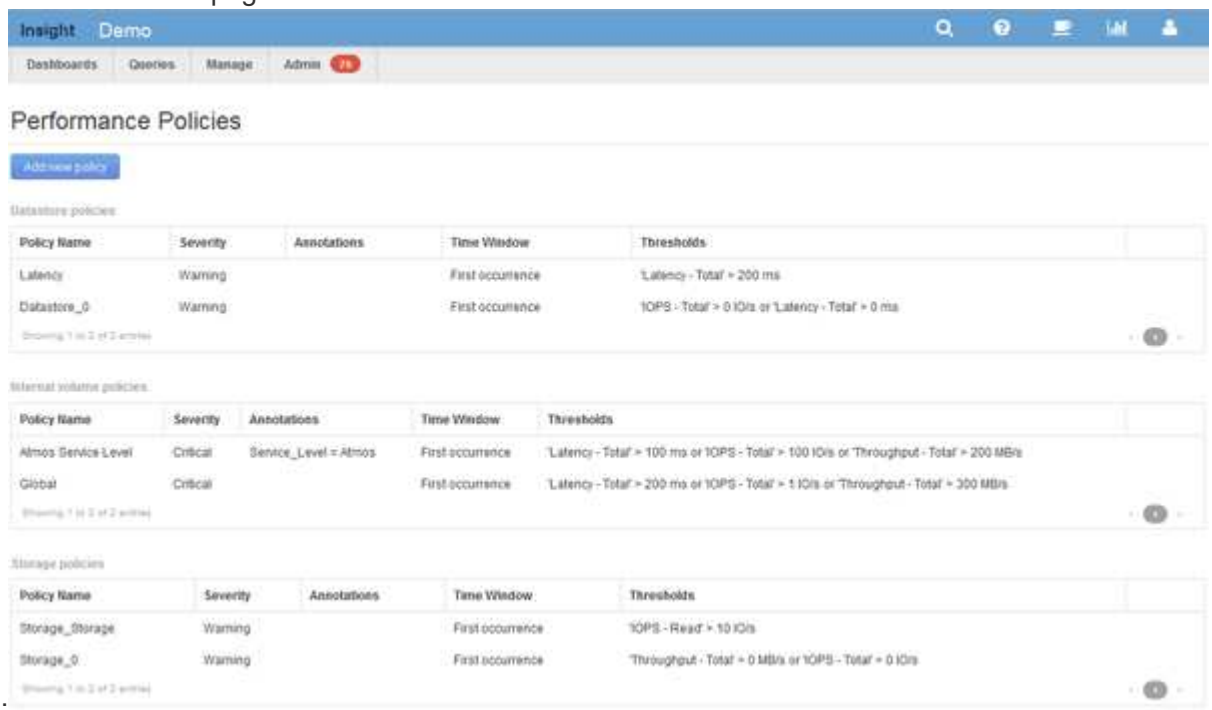
Creating performance policies

You create performance policies to set thresholds that trigger alerts to notify you about issues related to the resources in your network. For example, you can create a performance policy to alert you when the total utilization for storage pools is greater than 60%.

Steps

1. Open OnCommand Insight in your browser.
2. Select **Manage** > **Performance Policies**.

   The Performance Policies page is displayed.



   Policies are organized by object, and are evaluated in the order in which they appear in the list for that object.

3. Click **Add new policy**.

   The Add Policy dialog box is displayed.

4. In the **Policy name** field, enter a name for the policy.

   You must use a name that is different from all the other policy names for the object. For example, you cannot have two policies named “Latency” for an internal volume; however, you can have a “Latency” policy for an internal volume and another “Latency” policy for a different volume. The best practice is to always use a unique name for any policy, regardless of the object type.

5. From the **Apply to objects of type** list, select the type of object to which the policy applies.
6. From the **With annotation** list, select an annotation type, if applicable, and enter a value for the annotation in the **Value** box to apply the policy only to objects that have this particular annotation set.
7. If you selected **Port** as the object type, from the **Connected to** list, select what the port is connected to.
8. From the **Apply after a window of** list, select when an alert is raised to indicate a threshold violation.

   The First occurrence option triggers an alert when a threshold is exceeded on the first sample of data. All other options trigger an alert when the threshold is crossed once and is continuously crossed for at least the specified amount of time.

9. From the **With severity** list, select the severity for the violation.

10. By default, email alerts on policy violations will be sent to the recipients in the global email list. You can override these settings so that alerts for a particular policy are sent to specific recipients.
    - Click the link to open the recipients list, then click the **+** button to add recipients. Violation alerts for that policy will be sent to all recipients in the list.
11. Click the **any** link in the **Create alert if any of the following are true** section to control how alerts are triggered:
    - **any**

      This is the default setting, which creates alerts when any of the thresholds related to a policy are crossed.

    - **all**

      This setting creates an alert when all of the thresholds for a policy are crossed. When you select **all**, the first threshold that you create for a performance policy is referred to as the primary rule. You must ensure that the primary rule threshold is the violation that you are most concerned about for the performance policy.
12. In the **Create alert if** section, select a performance counter and an operator, and then enter a value to create a threshold.
13. Click **Add threshold** to add more thresholds.
14. To remove a threshold, click the trash can icon.
15. Select the **Stop processing further policies if alert is generated** check box if you want the policy to stop processing when an alert occurs.

    For example, if you have four policies for datastores, and the second policy is configured to stop processing when an alert occurs, the third and fourth policies are not processed while a violation of the second policy is active.

16. Click **Save**.

    The Performance Policies page displays, and the performance policy appears in the list of policies for the object type.

Performance policy evaluation precedence

The Performance Policies page groups policies by object type and Insight evaluates the policies in the order in which they appear in the object's performance policy list. You can change the order in which Insight evaluates policies in order to show the information that is most important to you in your network.

Insight evaluates all policies that are applicable to an object sequentially when performance data samples are taken into the system for that object; however, depending on annotations, not all policies apply to one group of objects. For example, suppose that internal volume has the following policies:

- Policy 1 (the Insight-supplied default policy)
- Policy 2 (with an annotation of "Service Level = Silver" with the **Stop processing further policies if alert is generated** option
- Policy 3 (with an annotation of"`Service Level = Gold`")

- Policy 4

For an internal volume tier with a Gold annotation, Insight evaluates Policy 1, ignores Policy 2, and then evaluates Policy 3 and Policy 4. For an unannotated tier, Insight evaluates by the order of the policies; thus, Insight evaluates only Policy 1 and Policy 4. For an internal volume tier with a Silver annotation, Insight evaluates Policy 1 and Policy 2; however, if an alert is triggered when the policy's threshold is crossed once and is continuously crossed for the window of time specified in the policy, then Insight no longer evaluates the other policies in the list while it evaluates the current counters for the object. When Insight captures the next set of performance samples for the object, it again begins to evaluate the performance policies for the object by filter and then order.

Changing the precedence of a performance policy

By default, Insight evaluates an object's policies sequentially. You can configure the order in which Insight evaluates performance policies. For example, if you have a policy configured to stop processing when a violation occurs for Gold Tier storage, you can place that policy first in the list and avoid seeing more generic violations for the same storage asset.

Steps

1. Open Insight in your browser.
2. From the **Manage** menu, select **Performance Policies**.

   The Performance Policies page displays.

3. Hover your cursor over a policy name in an object type's performance policy list.

   The precedence arrows appear to the right of the policy.

4. To move a policy up in the list, click the up arrow; to move a policy down in the list, click the down arrow.

   By default, new policies are added sequentially to an object's list of policies.

Editing performance policies

You can edit existing and default performance policies to change how Insight monitors the conditions of interest to you in your network. For example, you might want to change a policy's threshold.

Steps

1. Open Insight in your browser.
2. From the **Manage** menu, select **Performance Policies**.

   The Performance Policies page displays.

3. Hover your cursor over a policy name in an object's performance policy list.
4. Click .

The Edit Policy dialog box displays.

5. Make the required changes.

   If you change any option other than the policy name, Insight deletes all existing violations for that policy.

6. Click **Save.**

Deleting performance policies

You can delete a performance policy if you feel that it is no longer applicable to monitoring the objects in your network.

Steps

1. Open Insight in your browser.
2. From the **Manage** menu, select **Performance Policies**.

   The Performance Policies page displays.

3. Hover your cursor over the name of a policy in an object's performance policy list.
4. Click ✖.

   A message appears, asking if you want to delete the policy.

5. Click **OK**.

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.