Creating performance policies

OnCommand Insight

NetApp
September 19, 2024

Table of Contents

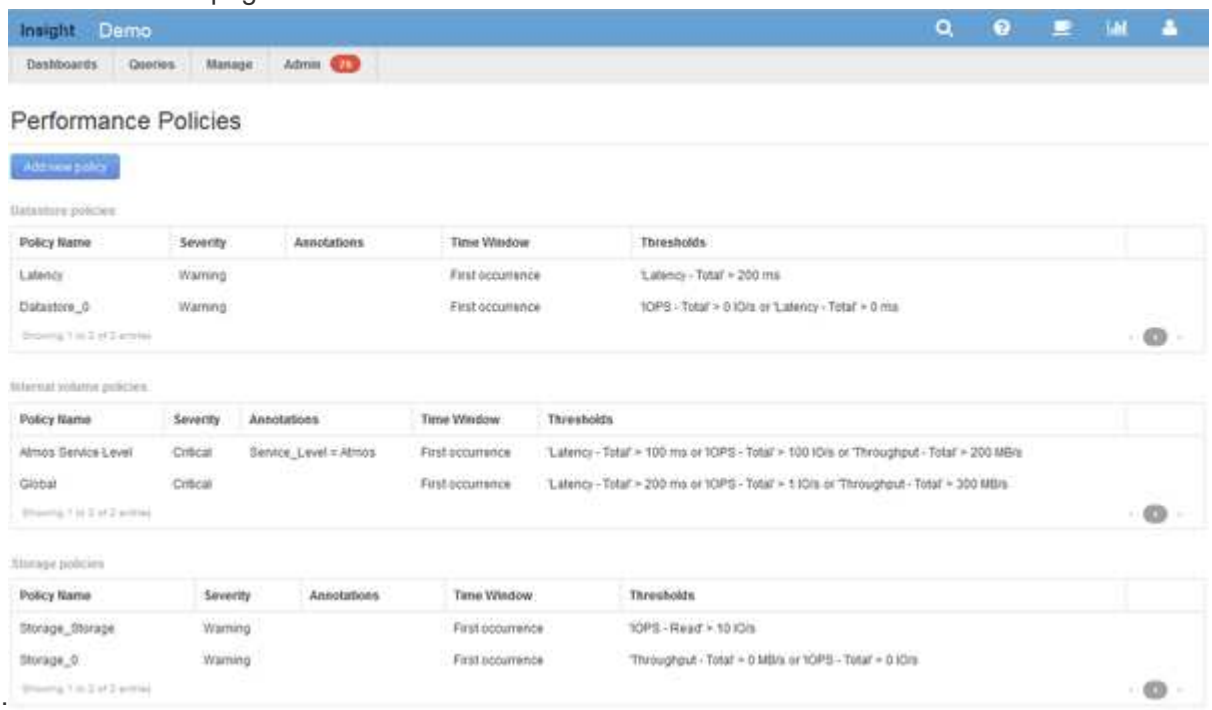
Creating performance policies

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.

Configuring performance and assure violation notifications

OnCommand Insight supports notifications for performance and assure violations. By default, Insight does not send notifications for these violations; you must configure Insight to send email, to send syslog messages to the syslog server, or to send SNMP notifications when a violation occurs.

Before you begin

You must have configured email, syslog, and SNMP sending methods for violations.

Steps

1. Click **Admin** > **Notifications**.
2. Click **Events**.
3. In the **Performance Violations events** or **Assure Violations events** section, click the list for the notification method (**Email**, **Syslog**, or **SNMP**) you want, and select the severity level (**Warning and above** or **Critical**) for the violation.
4. Click **Save**.

Monitoring the violations in your network

When Insight generates violations due to the thresholds set in performance policies, you can view them using the Violations Dashboard. The dashboard lists all the violations that occur in your network and enables you to locate and address issues.

Steps

1. Open OnCommand Insight in your browser.
2. On the Insight toolbar, click **Dashboards** and select **Violations Dashboard**.

   The Violations Dashboard displays.

3. You can use the **Violations By Policies** pie chart in the following ways:
   - You can position your cursor over any slice of a chart to display the percentage of the total violations that occurred for a particular policy or metric.
   - You can click a slice of a chart to “enlarge” it, which enables you to emphasize and study more carefully that slice by moving it away from the rest of the chart.
   - You can click the icon in the upper-right corner to display the pie chart in full screen mode, and click again to minimize the pie chart. A pie chart can contain a maximum of five slices; thus, if you have six policies that generate violations, Insight combines the fifth and sixth slices into an “Others” slice. Insight assigns the most violations to the first slice, the second most violations to the second slice, and so on.
4. You can use the **Violations History** chart in the following ways:
   - You can position your cursor over the chart to display the total number of violations that occurred at a particular time and the number that occurred out of the total for each specified metric.
   - You can click a legend label to remove the data associated with the legend from the chart.

     Click on the legend to display the data again.

   - You can click the icon in the upper-right corner to display the chart in full screen mode, and click again to minimize the pie chart.
5. You can use the **Violations Table** in the following ways:
   - You can click the icon in the upper-right corner to display the table in full screen mode, and click

again to minimize the pie chart.

If your window size is too small, then the Violations Table displays only three columns; however, when you click , additional columns (up to seven) display.

- You can display violations for a particular time period (**1h**, **3h**, **24h**, **3d**, **7d**, and **30d**), with Insight showing a maximum number of 1000 violations for the selected time period.
- You can use the **filter** box to show only the violations you want.
- You can change the sort order of the columns in a table to either ascending (up arrow) or descending (down arrow) by clicking the arrow in the column header; to return to the default sort order, click any other column header.

  By default, the table displays the violations in descending order.

- You can click a violation in the ID column to display the asset page for the duration of the violation.
- You can click the resource links (for example, storage pool and storage volume) in the Description column to display the asset pages associated with those resources.
- You can click the performance policy link in the Policy column to display the Edit Policy dialog box.

  You might want to adjust the thresholds for a policy if you feel it generates too few or too many violations.

- You can click a page number to browse through data by page if there is more data than fits on a single page.
- You can click to dismiss the violation.

Copyright information

Trademark information