Manage performance thresholds

Active IQ Unified Manager

NetApp
September 26, 2026

This PDF was generated from https://docs.netapp.com/us-en/active-iq-unified-manager/performance-checker/concept_manage_performance_thresholds.html on September 26, 2026. Always check docs.netapp.com for the latest.

Table of Contents

Manage performance thresholds . . . 1
- Manage performance thresholds in Active IQ Unified Manager . . . 1
- Use user-defined performance threshold policies in Active IQ Unified Manager . . . 1
- Respond to breached performance threshold policies in Active IQ Unified Manager . . . 3
- Understand performance counters tracked using thresholds in Active IQ Unified Manager . . . 3
  - Available performance counters . . . 3
- Understand combination threshold policy objects and counters in Active IQ Unified Manager . . . 6
- Create user-defined performance threshold policies in Active IQ Unified Manager . . . 6
- Assign performance threshold policies to storage objects in Active IQ Unified Manager . . . 8
- View performance threshold policies in Active IQ Unified Manager . . . 9
- Edit user-defined performance threshold policies in Active IQ Unified Manager . . . 9
- Remove performance threshold policies from storage objects in Active IQ Unified Manager . . . 10
- Understand performance threshold policy changes in Active IQ Unified Manager . . . 10
- Manage threshold policies when moving objects in Active IQ Unified Manager . . . 11
  - Threshold policy functionality during HA takeover and giveback . . . 11
  - Threshold policy functionality during aggregate relocation . . . 11
  - Threshold policy functionality during MetroCluster switchover . . . 11

Manage performance thresholds

Manage performance thresholds in Active IQ Unified Manager

Performance threshold policies enable you to determine the point at which Unified Manager generates an event to inform system administrators about issues that could be impacting workload performance. These threshold policies are known as *user-defined* performance thresholds.

This release supports user-defined, system-defined, and dynamic performance thresholds. With dynamic and system-defined performance thresholds, Unified Manager analyzes the workload activity to determine the appropriate threshold value. With user-defined thresholds, you can define the upper performance limits for many performance counters and for many storage objects.

System-defined performance thresholds and dynamic performance thresholds are set by Unified Manager and are not configurable. If you are receiving unnecessary events from any system-defined performance threshold policies, you can disable individual policies from the Event Setup page.

Use user-defined performance threshold policies in Active IQ Unified Manager

You set performance threshold policies on storage objects (for example, on aggregates and volumes) so that an event can be sent to the storage administrator to inform the administrator that the cluster is experiencing a performance issue.

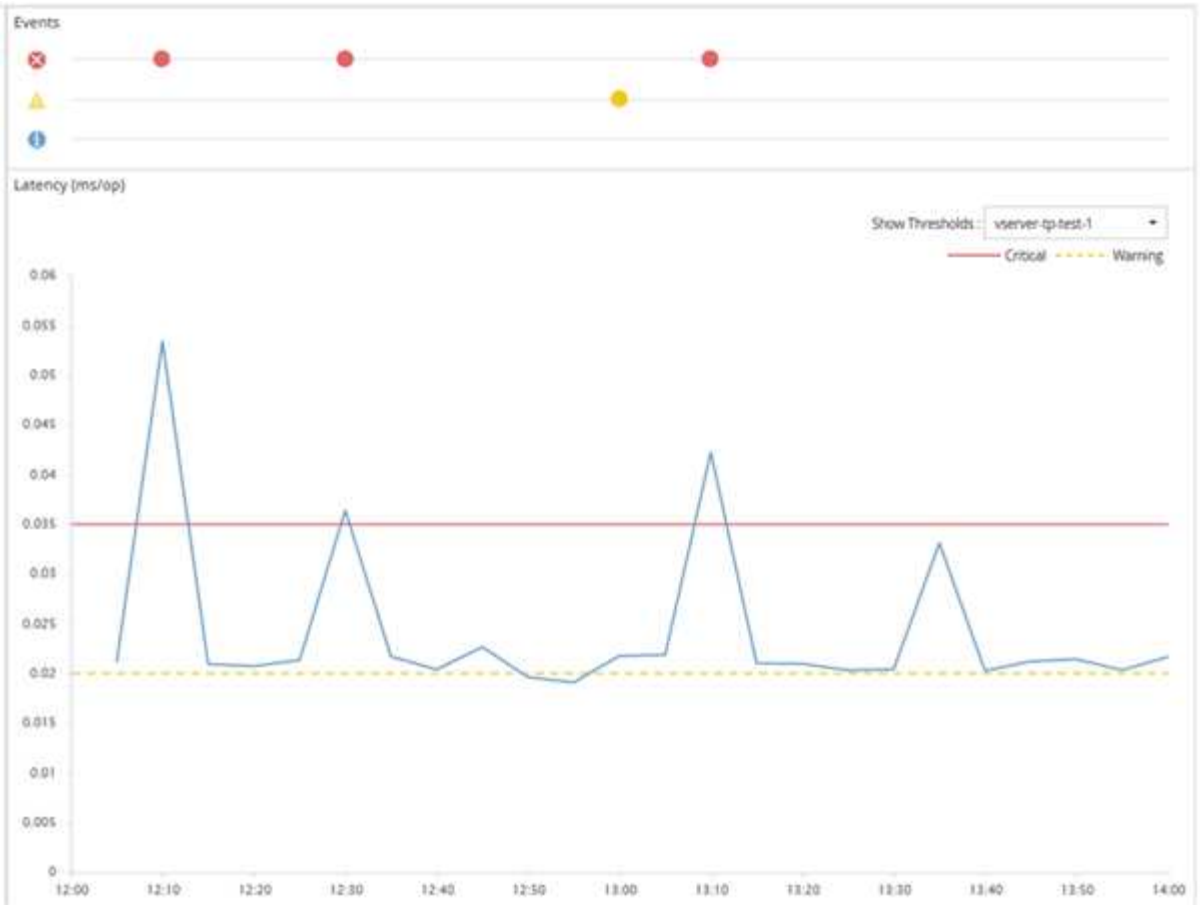
You create a performance threshold policy for a storage object by:

- Selecting a storage object
- Selecting a performance counter associated with that object
- Specifying values that define the performance counter upper limits that are considered warning and critical situations
- Specifying a time period that defines how long the counter must exceed the upper limit

For example, you can set a performance threshold policy on a volume so that you receive a critical event notification whenever IOPS for that volume exceeds 750 operations per second for 10 consecutive minutes. This same threshold policy can also specify that a warning event be sent when IOPS exceeds 500 operations per second for 10 minutes.

The current release provides thresholds that send events when a counter value exceeds the threshold setting. You cannot set thresholds that send events when a counter value falls below a threshold setting.

An example counter chart is shown here, indicating that a warning threshold (yellow icon) was breached at 1:00, and that a critical threshold (red icon) was breached at 12:10, 12:30, and 1:10:



A threshold breach must occur continuously for the specified duration. If the threshold dips below the limit values for any reason, a subsequent breach is considered the start of a new duration.

Some cluster objects and performance counters enable you to create a combination threshold policy that requires two performance counters to exceed their maximum limits before an event is generated. For example, you can create a threshold policy using the following criteria:

Cluster object	Performance counter	Warning threshold	Critical threshold	Duration
Volume	Latency	10 milliseconds	20 milliseconds	15 minutes
Aggregate	Utilization	65%	85%	

Threshold policies that use two cluster objects cause an event to be generated only when both conditions are breached. For example, using the threshold policy defined in the table:

If volume latency is averaging…	And aggregate disk utilization is…	Then…
15 milliseconds	50%	No event is reported.
15 milliseconds	75%	A Warning event is reported.
25 milliseconds	75%	A Warning event is reported.
25 milliseconds	90%	A Critical event is reported.

Respond to breached performance threshold policies in Active IQ Unified Manager

When a counter value exceeds its defined performance threshold value for the amount of time specified in the duration, the threshold is breached and an event is reported.

The event causes the following actions to be initiated:

- The event is displayed in the Dashboard, the Performance Cluster Summary page, the Events page, and the object-specific Performance Inventory page.
- (optional) An email alert about the event can be sent to one or more email recipients, and an SNMP trap can be sent to a trap receiver.
- (optional) A script can be executed to automatically modify or update storage objects.

The first action is always executed. You configure whether the optional actions are performed in the Alert Setup page. You can define unique actions depending on whether a Warning or a Critical threshold policy is breached.

After a performance threshold policy breach has occurred on a storage object, no further events are generated for that policy until the counter value goes below the threshold value, at which point the duration resets for that limit. While the threshold continues to be exceeded, the end time of the event is continually updated to reflect that this event is ongoing.

A threshold event captures, or freezes, the information related to severity and policy definition so that unique threshold information displays with the event, even if the threshold policy is modified in the future.

Understand performance counters tracked using thresholds in Active IQ Unified Manager

Some common performance counters, such as IOPS and MB/s, can have thresholds set for all storage objects. There are other counters that can have thresholds set for only certain storage objects.

Available performance counters

Storage object	Performance counter	Description
Cluster	IOPS	Average number of input/output operations the cluster processes per second.
	MB/s	Average number of megabytes of data transferred to and from this cluster per second.

Storage object	Performance counter	Description
Node	IOPS	Average number of input/output operations the node processes per second.
	MB/s	Average number of megabytes of data transferred to and from this node per second.
	Latency	Average number of milliseconds the node takes to respond to application requests.
	Utilization	Average percentage of the node's CPU and RAM that is being used.
	Performance Capacity Used	Average percentage of performance capacity that is being consumed by the node.
	Performance Capacity Used - Takeover	Average percentage of performance capacity that is being consumed by the node, plus the performance capacity of its partner node.
Aggregate	IOPS	Average number of input/output operations the aggregate processes per second.
	MB/s	Average number of megabytes of data transferred to and from this aggregate per second.
	Latency	Average number of milliseconds the aggregate takes to respond to application requests.
	Utilization	Average percentage of the aggregate's disks that are being used.
	Performance Capacity Used	Average percentage of performance capacity that is being consumed by the aggregate.
Storage VM	IOPS	Average number of input/output operations the SVM processes per second.
	MB/s	Average number of megabytes of data transferred to and from this SVM per second.
	Latency	Average number of milliseconds the SVM takes to respond to application requests.

Storage object	Performance counter	Description
Volume	IOPS	Average number of input/output operations the volume processes per second.
	MB/s	Average number of megabytes of data transferred to and from this volume per second.
	Latency	Average number of milliseconds the volume takes to respond to application requests.
	Cache miss ratio	Average percentage of read requests from client applications that are returned from the volume instead of being returned from cache.
LUN	IOPS	Average number of input/output operations the LUN processes per second.
	MB/s	Average number of megabytes of data transferred to and from this LUN per second.
	Latency	Average number of milliseconds the LUN takes to respond to application requests.
Namespace	IOPS	Average number of input/output operations the namespace processes per second.
	MB/s	Average number of megabytes of data transferred to and from this namespace per second.
	Latency	Average number of milliseconds the namespace takes to respond to application requests.
Port	Bandwidth utilization	Average percentage of the port's available bandwidth that is being used.
	MB/s	Average number of megabytes of data transferred to and from this port per second.
Network Interface (LIF)	MB/s	Average number of megabytes of data transferred to and from this LIF per second.

Understand combination threshold policy objects and counters in Active IQ Unified Manager

Only some performance counters can be used together in combination policies. When primary and secondary performance counters are specified, both performance counters must exceed their maximum limits before an event is generated.

Primary storage object and counter	Secondary storage object and counter
Volume Latency	Volume IOPS
	Volume MB/s
	Aggregate Utilization
	Aggregate Performance Capacity Used
	Node Utilization
	Node Performance Capacity Used
	Node Performance Capacity Used - Takeover
LUN Latency	LUN IOPS
	LUN MB/s
	Aggregate Utilization
	Aggregate Performance Capacity Used
	Node Utilization
	Node Performance Capacity Used
	Node Performance Capacity Used - Takeover

When a volume combination policy is applied to a FlexGroup volume, instead of to a FlexVol volume, only the “Volume IOPS” and “Volume MB/s” attributes can be selected as the secondary counter. If the threshold policy contains one of the node or aggregate attributes, then the policy will not be applied to the FlexGroup volume, and you will receive an error message describing this case. This is because FlexGroup volumes can exist on more than one node or aggregate.

Create user-defined performance threshold policies in Active IQ Unified Manager

You create performance threshold policies for storage objects so that notifications are sent when a performance counter exceeds a specific value. The event notification identifies that the cluster is experiencing a performance issue.

Before you begin

You must have the Application Administrator role.

You create performance threshold policies by entering the threshold values on the Create Performance Threshold Policy page. You can create new policies by defining all the policy values in this page, or you can make a copy of an existing policy and change the values in the copy (called *cloning*).

Valid threshold values are 0.001 through 10,000,000 for numbers, 0.001-100 for percentages, and 0.001-200 for Performance Capacity Used percentages.

The current release provides thresholds that send events when a counter value exceeds the threshold setting. You cannot set thresholds that send events when a counter value falls below a threshold setting.

Steps

1. In the left navigation pane, select **Event Thresholds** > **Performance**.

   The Performance Thresholds page is displayed.

2. Click the appropriate button depending on whether you want to build a new policy or if you want to clone a similar policy and modify the cloned version.

To…	Click…
Create a new policy	**Create**
Clone an existing policy	Select an existing policy and click **Clone**

   The Create Performance Threshold Policy page or Clone Performance Threshold Policy page is displayed.

3. Define the threshold policy by specifying the performance counter threshold values you want to set for specific storage objects:

   a. Select the storage object type and specify a name and description for the policy.

   b. Select the performance counter to be tracked and specify the limit values that define Warning and Critical events.

      You must define at least one Warning or one Critical limit. You do not need to define both types of limits.

   c. Select a secondary performance counter, if required, and specify the limit values for Warning and Critical events.

      Including a secondary counter requires that both counters exceed the limit values before the threshold is breached and an event is reported. Only certain objects and counters can be configured using a combination policy.

   d. Select the duration of time for which the limit values must be breached for an event to be sent.

   When cloning an existing policy, you must enter a new name for the policy.

4. Click **Save** to save the policy.

   You are returned to the Performance Thresholds page. A success message at the top of the page confirms that the threshold policy was created and provides a link to the Inventory page for that object type so that you can apply the new policy to storage objects immediately.

If you want to apply the new threshold policy to storage objects at this time, you can click the **Go to object_type now** link to go to the Inventory page.

Assign performance threshold policies to storage objects in Active IQ Unified Manager

You assign a user-defined performance threshold policy to a storage object so that Unified Manager reports an event if the value of the performance counter exceeds the policy setting.

Before you begin

You must have the Application Administrator role.

The performance threshold policy, or policies, that you want to apply to the object must exist.

You can apply only one performance policy at a time to an object, or to a group of objects.

You can assign a maximum of three threshold policies to each storage object. When assigning policies to multiple objects, if any of the objects already has the maximum number of policies assigned, Unified Manager performs the following actions:

- Applies the policy to all of the selected objects that have not reached their maximum
- Ignores the objects that have reached the maximum number of policies
- Displays a message that the policy was not assigned to all objects

Steps

1. From the Performance inventory page of any storage object, select the object or objects to which you want to assign a threshold policy:

To assign thresholds to…	Click…
A single object	The check box at the left of that object.
Multiple objects	The check box at the left of each object.
All objects on the page	The ☐▾ drop-down box, and choose **Select all objects on this page**.
All objects of the same type	The ☐▾ drop-down box, and choose **Select all objects**.

   You can use the sorting and filtering functionality to refine the list of objects on the inventory page to make it easier to apply threshold policies to many objects.

2. Make your selection, and then click **Assign Performance Threshold Policy**.

   The Assign Performance Threshold Policy page is displayed, showing a list of threshold policies that exist for that specific type of storage object.

3. Click each policy to display the details of the performance threshold settings to verify that you have selected the correct threshold policy.
4. After you have selected the appropriate threshold policy, click **Assign Policy**.

   A success message at the top of the page confirms that the threshold policy was assigned to the object or objects, and provides a link to the Alerting page so that you can configure alert settings for this object and policy.

If you want to have alerts sent over email, or as an SNMP trap, to notify you that a particular performance event has been generated, you must configure the alert settings in the Alert Setup page.

View performance threshold policies in Active IQ Unified Manager

You can view all of the currently defined performance threshold policies from the Performance Thresholds page.

The list of threshold policies is sorted alphabetically by policy name, and it includes policies for all types of storage objects. You can click a column header to sort the policies by that column. If you are looking for a specific policy, use the filter and search mechanisms to refine the list of threshold policies that appear in the inventory list.

You can hover your cursor over the Policy Name and the Condition name to see the configuration details of the policy. Additionally, you can use the provided buttons to create, clone, edit, and delete user-defined threshold policies.

Step

1. In the left navigation pane, select **Event Thresholds** > **Performance**.

   The Performance Thresholds page is displayed.

Edit user-defined performance threshold policies in Active IQ Unified Manager

You can edit the threshold settings for existing performance threshold policies. This can be useful if you find that you are receiving too many or too few alerts for certain threshold conditions.

Before you begin

You must have the Application Administrator role.

You cannot change the policy name or the type of storage object that is being monitored for existing threshold policies.

Steps

1. In the left navigation pane, select **Event Thresholds** > **Performance**.

   The Performance Thresholds page displays.

2. Select the threshold policy that you want to change and click **Edit**.

   The Edit Performance Threshold Policy page is displayed.

3. Make your changes to the threshold policy and click **Save**.

   You are returned to the Performance Thresholds page.

After they are saved, changes are updated immediately on all storage objects that use the policy.

Depending on the type of changes that you made to the policy, you may want to review the alert settings configured for the objects that use the policy in the Alert Setup page.

Remove performance threshold policies from storage objects in Active IQ Unified Manager

You can remove a user-defined performance threshold policy from a storage object when you no longer want Unified Manager to monitor the value of the performance counter.

Before you begin

You must have the Application Administrator role.

You can remove only one policy at a time from a selected object.

You can remove a threshold policy from multiple storage objects by selecting more than one object in the list.

Steps

1. From the **inventory** page of any storage object, select one or more objects that have at least one performance threshold policy applied.

To clear thresholds from…	Do this…
A single object	Select the check box at the left of that object.
Multiple objects	Select the check box at the left of each object.
All objects on the page	Click in the column header.

2. Click **Clear Performance Threshold Policy**.

   The Clear Threshold Policy page displays, showing a list of threshold policies that are currently assigned to the storage objects.

3. Select the threshold policy you want to remove from the objects and click **Clear Policy**.

   When you select a threshold policy, the details of the policy display so that you can confirm that you have selected the appropriate policy.

Understand performance threshold policy changes in Active IQ Unified Manager

If you adjust the counter value or duration of an existing performance threshold policy, the policy change is applied to all storage objects that use the policy. The new setting takes place immediately, and Unified Manager begins to compare performance counter values to the new threshold settings for all newly collected performance data.

If any active events exist for objects that are using the changed threshold policy, the events are marked as obsolete, and the threshold policy begins monitoring the counter as a newly defined threshold policy.

When viewing the counter on which the threshold has been applied in the Counter Charts Detailed View, the critical and warning threshold lines reflect the current threshold settings. The original threshold settings do not appear on this page even if you view historical data when the old threshold setting was in effect.

Because older threshold settings do not appear in the Counter Charts Detailed View, you might see historical events that appear below the current threshold lines.

Manage threshold policies when moving objects in Active IQ Unified Manager

Because performance threshold policies are assigned to storage objects, if you move an object, all assigned threshold policies remain attached to the object after the move is completed. For example, if you move a volume or LUN to a different aggregate, the threshold policies are still active for the volume or LUN on the new aggregate.

If a secondary counter condition exists for the threshold policy (a combination policy)--for example, if an additional condition is assigned to an aggregate or a node—the secondary counter condition is applied to the new aggregate or node to which the volume or LUN has been moved.

If any new active events exist for objects that are using the changed threshold policy, the events are marked as obsolete, and the threshold policy begins monitoring the counter as a newly defined threshold policy.

A volume move operation causes ONTAP to send an informational change event. A change event icon appears in the Events timeline on the Performance Explorer page and the Workload Analysis page to indicate the time when the move operation was completed.

If you move an object to a different cluster, the user-defined threshold policy is removed from the object. If required, you must assign a threshold policy to the object after the move operation is completed. Dynamic and system-defined threshold policies, however, are applied automatically to an object after it has moved to a new cluster.

Threshold policy functionality during HA takeover and giveback

When a takeover or giveback operation occurs in a high-availability (HA) configuration, objects that are moved from one node to the other node retain their threshold policies in the same manner as in the manual move operations. Because Unified Manager checks for cluster configuration changes every 15 minutes, the impact of the switchover to the new node is not identified until the next poll of the cluster configuration.

If both a takeover and giveback operation occur within the 15-minute configuration change collection period, you might not see the performance statistics move from one node to the other node.

Threshold policy functionality during aggregate relocation

If you move an aggregate from one node to another node using the `aggregate relocation start` command, both single and combination threshold policies are retained on all objects, and the node portion of the threshold policy is applied to the new node.

Threshold policy functionality during MetroCluster switchover

Objects that move from one cluster to another cluster in a MetroCluster configuration do not retain their user-defined threshold policy settings. If required, you can apply threshold policies on the volumes and LUNs that have moved to the partner cluster. After an object has moved back to its original cluster, the user-defined threshold policy is reapplied automatically.

For information, see Volume behavior during switchover and switchback.

Copyright information

Copyright © 2026 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.