



# **Monitor cluster performance with System Manager**

**ONTAP 9**

NetApp  
April 06, 2024

This PDF was generated from [https://docs.netapp.com/us-en/ontap/task\\_cp\\_monitor\\_cluster\\_performance\\_sm.html](https://docs.netapp.com/us-en/ontap/task_cp_monitor_cluster_performance_sm.html) on April 06, 2024. Always check docs.netapp.com for the latest.

# Table of Contents

- Monitor cluster performance with System Manager . . . . . 1
  - Monitor cluster performance using System Manager. . . . . 1
  - View performance on cluster dashboard . . . . . 1
  - Identify hot volumes and other objects. . . . . 1
  - Modify QoS. . . . . 2
  - Monitor risks. . . . . 2
  - System Manager insights . . . . . 4
  - Gain insights to help optimize your system . . . . . 8
  - Configure native FPolicy . . . . . 10

# Monitor cluster performance with System Manager

## Monitor cluster performance using System Manager

The topics in this section show you how to manage cluster health and performance with System Manager in ONTAP 9.7 and later releases.

You can monitor cluster performance by viewing information about your system on the System Manager Dashboard. The Dashboard displays information about important alerts and notifications, the efficiency and capacity of storage tiers and volumes, the nodes that are available in a cluster, the status of the nodes in an HA pair, the most active applications and objects, and the performance metrics of a cluster or a node.

The Dashboard lets you determine the following information:

- **Health:** How healthy is the cluster?
- **Capacity:** What capacity is available on the cluster?
- **Performance:** How well is the cluster performing, based on latency, IOPS, and throughput?
- **Network:** How is the network configured with hosts and storage objects, such as ports, interfaces, and storage VMs?

In the Health and Capacity overviews, you can click [→](#) to view additional information and perform tasks.

In the Performance overview, you can view metrics based on the hour, the day, the week, the month, or the year.

In the Network overview, the number of each object in the network is displayed (for example, "8 NVMe/FC ports"). You can click on the numbers to view details about each network object.

## View performance on cluster dashboard

Use the dashboard to make informed decisions about workloads you might want to add or move. You can also look at peak usage times to plan for potential changes.

The performance values refresh every 3 seconds and the performance graph refreshes every 15 seconds.

### Steps

1. Click **Dashboard**.
2. Under **Performance**, select the interval.

## Identify hot volumes and other objects

Accelerate your cluster performance by identifying the frequently accessed volumes (hot volumes) and data (hot objects).



Beginning in ONTAP 9.10.1, you can use the Activity Tracking feature in File System Analytics to monitor hot objects in a volume.


### Steps

1. Click **Storage > Volumes**.
2. Filter the IOPS, latency, and throughput columns to view the frequently accessed volumes and data.

## Modify QoS

Beginning with ONTAP 9.8, when you provision storage, [Quality of Service \(QoS\)](#) is enabled by default. You can disable QoS or choose a custom QoS policy during the provisioning process. You can also modify QoS after your storage has been provisioned.

### Steps

1. In System Manager, select **Storage** then **Volumes**.
2. Next to the volume for which you want to modify QoS, select  then **Edit**.

## Monitor risks

Beginning with ONTAP 9.10.0, you can use System Manager to monitor the risks reported by Active IQ Digital Advisor. Beginning with ONTAP 9.10.1, you can use System Manager to also acknowledge the risks.

NetApp Active IQ Digital Advisor reports opportunities to reduce risk and improve the performance and efficiency of your storage environment. With System Manager, you can learn about risks reported by Active IQ and receive actionable intelligence that helps you administer storage and achieve higher availability, improved security, and better storage performance.

### Link to your Active IQ account

To receive information about risks from Active IQ, you should first link to your Active IQ account from System Manager.

### Steps

1. In System Manager, click **Cluster > Settings**.
2. Under **Active IQ Registration**, click **Register**.
3. Enter your credentials for Active IQ.
4. After your credentials are authenticated, click **Confirm to link Active IQ with System Manager**.

### View the number of risks

Beginning with ONTAP 9.10.0, you can view from the dashboard in System Manager the number of risks reported by Active IQ.

### Before you begin

You must establish a connection from System Manager to your Active IQ account. Refer to [Link to your Active IQ account](#).

### Steps

1. In System Manager, click **Dashboard**.

2. In the **Health** section, view the number of reported risks.



You can view more detailed information about each risk by clicking the message showing the number of risks. See [View details of risks](#).

## View details of risks

Beginning with ONTAP 9.10.0, you can view from System Manager how the risks reported by Active IQ are categorized by impact areas. You can also view detailed information about each reported risk, its potential impact on your system, and corrective actions you can take.

### Before you begin

You must establish a connection from System Manager to your Active IQ account. Refer to [Link to your Active IQ account](#).

### Steps

1. Click **Events > All Events**.
2. In the **Overview** section, under **Active IQ Suggestions**, view the number of risks in each impact area category. The risk categories include:
  - Performance & efficiency
  - Availability & protection
  - Capacity
  - Configuration
  - Security
3. Click on the **Active IQ Suggestions** tab to view information about each risk, including the following:
  - Level of impact to your System
  - Category of the risk
  - Nodes that are affected
  - Type of mitigation needed
  - Corrective actions you can take

## Acknowledge risks

Beginning with ONTAP 9.10.1, you can use System Manager to acknowledge any of the open risks.

### Steps

1. In System Manager, display the list of risks by performing the procedure in [View details of risks](#).
2. Click on the risk name of an open risk that you want to acknowledge.
3. Enter information into the following fields:
  - Reminder (date)
  - Justification
  - Comments
4. Click **Acknowledge**.



After you acknowledge a risk, it takes a few minutes for the change to be reflected in the list of Active IQ suggestions.

## Unacknowledge risks

Beginning with ONTAP 9.10.1, you can use System Manager to unacknowledge any risk that was previously acknowledged.

### Steps

1. In System Manager, display the list of risks by performing the procedure in [View details of risks](#).
2. Click on the risk name of an acknowledged risk that you want to unacknowledge.
3. Enter information into the following fields:
  - Justification
  - Comments
4. Click **Unacknowledge**.



After you unacknowledge a risk, it takes a few minutes for the change to be reflected in the list of Active IQ suggestions.

## System Manager insights

Beginning with ONTAP 9.11.1, System Manager displays *insights* that help you optimize the performance and security of your system.



To view, customize, and respond to insights, refer to [Gain insights to help optimize your system](#)

## Capacity insights

System Manager can display the following insights in response to capacity conditions in your system:

Insight	Severity	Condition	Fixes
Local tiers are lacking space	Remediate risks	One or more local tiers are more than 95% full and quickly growing. Existing workloads might be unable to grow, or in extreme cases, existing workloads might run out of space and fail.	<b>Recommended fix:</b> Perform one of following options. <ul style="list-style-type: none"><li>• Clear the volume recovery queue.</li><li>• Enable thin provisioning on thick provisioned volumes to free up trapped storage.</li><li>• Move volumes to another local tier.</li><li>• Delete unneeded Snapshot copies.</li><li>• Delete unneeded directories or files in the volumes.</li><li>• Enable Fabric Pool to tier the data to the cloud.</li></ul>

Applications are lacking space	Needs attention	One or more volumes are more than 95% full, but they do not have autogrow enabled.	<b>Recommended:</b> Enable autogrow up to 150% of current capacity.  <b>Other options:</b> <ul style="list-style-type: none"> <li>• Reclaim space by deleting Snapshot copies.</li> <li>• Resize the volumes.</li> <li>• Delete directories or files.</li> </ul>
FlexGroup volume's capacity is imbalanced	Optimize storage	The size of the constituent volumes of one or more FlexGroup volumes has grown unevenly over time, leading to an imbalance in capacity usage. If the constituent volumes become full, write failures could occur.	<b>Recommended:</b> Rebalance the FlexGroup volumes.
Storage VMs are running out of capacity	Optimize storage	One or more storage VMs are near their maximum capacity. You will not be able to provision more space for new or existing volumes if the storage VMs reach maximum capacity.	<b>Recommended:</b> If possible, increase the maximum capacity limit of the storage VM.

## Security insights

System Manager can display the following insights in response to conditions that might jeopardize the security of your data or your system.

Insight	Severity	Condition	Fixes
Volumes are still in anti-ransomware learning mode	Needs attention	One or more volumes have been in the anti-ransomware learning mode for 90 days.	<b>Recommended:</b> Enable the anti-ransomware active mode for those volumes.

Automatic deletion of Snapshot copies is enabled on volumes	Needs attention	Snapshot auto-deletion is enabled on one or more volumes.	<b>Recommended:</b> Disable the automatic deletion of Snapshot copies. Otherwise, in case of a ransomware attack, data recovery for these volumes might not be possible.
Volumes don't have Snapshot policies	Needs attention	One or more volumes don't have an adequate Snapshot policy attached to them.	<b>Recommended:</b> Attach a Snapshot policy to volumes that don't have one. Otherwise, in case of a ransomware attack, data recovery for these volumes might not be possible.
Native FPolicy is not configured	Best practice	Native FPolicy is not configured on one or more NAS storage VMs.	<b>Recommended: IMPORTANT:</b> Blocking extensions might lead to unexpected results. Beginning in 9.11.1, you can enable native FPolicy for storage VMs, which blocks over 3000 file extensions known to be used for ransomware attacks. <a href="#">Configure native FPolicy</a> in NAS storage VMs to control the file extensions that are allowed or not allowed to be written on volumes in your environment.
Telnet is enabled	Best practice	Secure Shell (SSH) should be used for secure remote access.	<b>Recommended:</b> Disable Telnet and use SSH for secure remote access.
Too few NTP servers are configured	Best practice	The number of servers configured for NTP is less than 3.	<b>Recommended:</b> Associate at least three NTP servers with the cluster. Otherwise, problems can occur with the synchronization of the cluster time.
Remote Shell (RSH) is enabled	Best practice	Secure Shell (SSH) should be used for secure remote access.	<b>Recommended:</b> Disable RSH and use SSH for secure remote access.
Login banner isn't configured	Best practice	Login messages are not configured either for the cluster, for the storage VM, or for both.	<b>Recommended:</b> Setup the login banners for the cluster and the storage VM and enable their use.
AutoSupport is using a nonsecure protocol	Best practice	AutoSupport is not configured to communicate via HTTPS.	<b>Recommended:</b> It is strongly recommended to use HTTPS as the default transport protocol to send AutoSupport messages to technical support.



Default admin user is not locked	Best practice	Nobody has logged in using a default administrative account (admin or diag), and these accounts are not locked.	<b>Recommended:</b> Lock default administrative accounts when they are not being used.
Secure Shell (SSH) is using nonsecure ciphers	Best practice	The current configuration uses nonsecure CBC ciphers.	<b>Recommended:</b> You should allow only secure ciphers on your web server to protect secure communication with your visitors. Remove ciphers that have names containing "cbc", such as "ais128-cbc", "aes192-cbc", "aes256-cbc", and "3des-cbc".
Global FIPS 140-2 compliance is disabled	Best practice	Global FIPS 140-2 compliance is disabled on the cluster.	<b>Recommended:</b> For security reasons, you should enable Global FIPS 140-2 compliant cryptography to ensure ONTAP can safely communicate with external clients or server clients.
Volumes aren't being monitored for ransomware attacks	Needs attention	Anti-ransomware is disabled on one or more volumes.	<b>Recommended:</b> Enable anti-ransomware on the volumes. Otherwise, you might not notice when volumes are being threatened or under attack.
Storage VMs aren't configured for anti-ransomware	Best practice	One or more storage VMs aren't configured for anti-ransomware protection.	<b>Recommended:</b> Enable anti-ransomware on the storage VMs. Otherwise, you might not notice when storage VMs are being threatened or under attack.

## Configuration insights

System Manager can display the following insights in response to concerns about the configuration of your system.

Insight	Severity	Condition	Fixes
Cluster isn't configured for notifications	Best practice	Email, webhooks, or an SNMP trap host is not configured to let you receive notifications about problems with the cluster.	<b>Recommended:</b> Configure notifications for the cluster.

Cluster isn't configured for automatic updates.	Best practice	The cluster hasn't been configured to receive automatic updates for the latest disk qualification package, disk firmware, shelf firmware, and SP/BMC firmware files when they are available.	<b>Recommended:</b> Enable this feature.
Cluster firmware isn't up-to-date	Best practice	Your system doesn't have the latest update to the firmware which could have improvements, security patches, or new features that help secure the cluster for better performance.	<b>Recommended:</b> Update the ONTAP firmware.

## Gain insights to help optimize your system

With System Manager, you can view insights that help you optimize your system.

### About this task

Beginning with ONTAP 9.11.0, you can view insights in System Manager that help you optimize the capacity and security compliance of your system.

Beginning with ONTAP 9.11.1, you can view additional insights that help you optimize the capacity, security compliance, and configuration of your system.



**Blocking extensions might lead to unexpected results.** Beginning with ONTAP 9.11.1, you can enable native FPolicy for storage VMs using System Manager. You might receive a System Manager Insight message recommending that you [configure native FPolicy](#) for a storage VM.

With FPolicy Native Mode, you can allow or disallow specific file extensions. System Manager recommends over 3000 disallowed file extensions that have been used in past ransomware attacks. Some of these extensions might be used by legitimate files in your environment and blocking them might lead to unexpected issues.

Therefore, it is strongly advised that you modify the list of extensions to meet the needs of your environment. Refer to [How to remove a file extension from a native FPolicy configuration created by System Manager using System Manager to recreate the policy](#).

To learn more about native FPolicy, see [FPolicy configuration types](#).

Based on best practices, these insights are displayed on one page from which you can initiate immediate actions to optimize your system. For more detail about each insight, see [System Manager insights](#).





## View optimization insights

### Steps

1. In System Manager, click **Insights** in the left-hand navigation column.

The **Insights** page shows groups of insights. Each group of insights might contain one or more insights. The following groups are displayed:

- Needs your attention
  - Remediate risks
  - Optimize your storage
2. (Optional) Filter the insights that are displayed by clicking these buttons in the upper-right corner of the page:

-  Displays the security-related insights.
-  Displays the capacity-related insights.
-  Displays the configuration-related insights.
-  Displays all of the insights.

## Respond to insights to optimize your system

In System Manager, you can respond to insights by either dismissing them, exploring different ways to remediate the problems, or initiating the process to fix the problems.

### Steps

1. In System Manager, click **Insights** in the left-hand navigation column.
2. Hover over an insight to reveal the buttons to perform the following actions:
  - **Dismiss:** Remove the insight from the view. To “undismiss” the insight, refer to [Customize the settings for insights](#).
  - **Explore:** Find out various ways to remediate the problem mentioned in the insight. This button appears only if there is more than one method of remediation.
  - **Fix:** Initiate the process of remediating the problem mentioned in the insight. You will be asked to confirm whether you want to take the action needed to apply the fix.




Some of these actions can be initiated from other pages in System Manager, but the **Insights** page helps you streamline your day-to-day tasks by allowing you to initiate these action from this one page.

## Customize the settings for insights

You can customize which insights you will be notified about in System Manager.

## Steps

1. In System Manager, click **Insights** in the left-hand navigation column.
2. In the upper-right corner of the page, click , then select **Settings**.
3. On the **Settings** page, ensure there is a check in the check boxes next to the insights you want to be notified about. If you previously dismissed an insight, you can “undismiss” it by ensuring a check is in its check box.
4. Click **Save**.

## Export the insights as a PDF file

You can export all applicable insights as a PDF file.

## Steps

1. In System Manager, click **Insights** in the left-hand navigation column.
2. In the upper-right corner of the page, click , then select **Export**.

## Configure native FPolicy

Beginning with ONTAP 9.11.1, when you receive a System Manager Insight that suggests implementing native FPolicy, you can configure it on your storage VMs and volumes.

### Before you begin

When you access System Manager Insights, under **Apply best practices**, you might receive a message saying that native FPolicy is not configured.

To learn more about FPolicy configuration types, refer to [FPolicy configuration types](#).

## Steps

1. In System Manager, click **Insights** in the left-hand navigation column.
2. Under **Apply best practices**, locate **Native FPolicy is not configured**.
3. Read the following message before taking action:



**Blocking extensions might lead to unexpected results.** Beginning with ONTAP 9.11.1, you can enable native FPolicy for storage VMs using System Manager. With FPolicy Native Mode, you can allow or disallow specific file extensions. System Manager recommends over 3000 disallowed file extensions that have been used in past ransomware attacks. Some of these extensions might be used by legitimate files in your environment and blocking them might lead to unexpected issues.

Therefore, it is strongly advised that you modify the list of extensions to meet the needs of your environment. Refer to [How to remove a file extension from a native FPolicy configuration created by System Manager using System Manager to recreate the policy](#).

4. Click **Fix**.
5. Select the storage VMs to which you want to apply the native FPolicy.
6. For each storage VM, select the volumes that will receive the native FPolicy.
7. Click **Configure**.

## 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.