



Analyze wellness attributes

Digital Advisor

NetApp

February 05, 2026

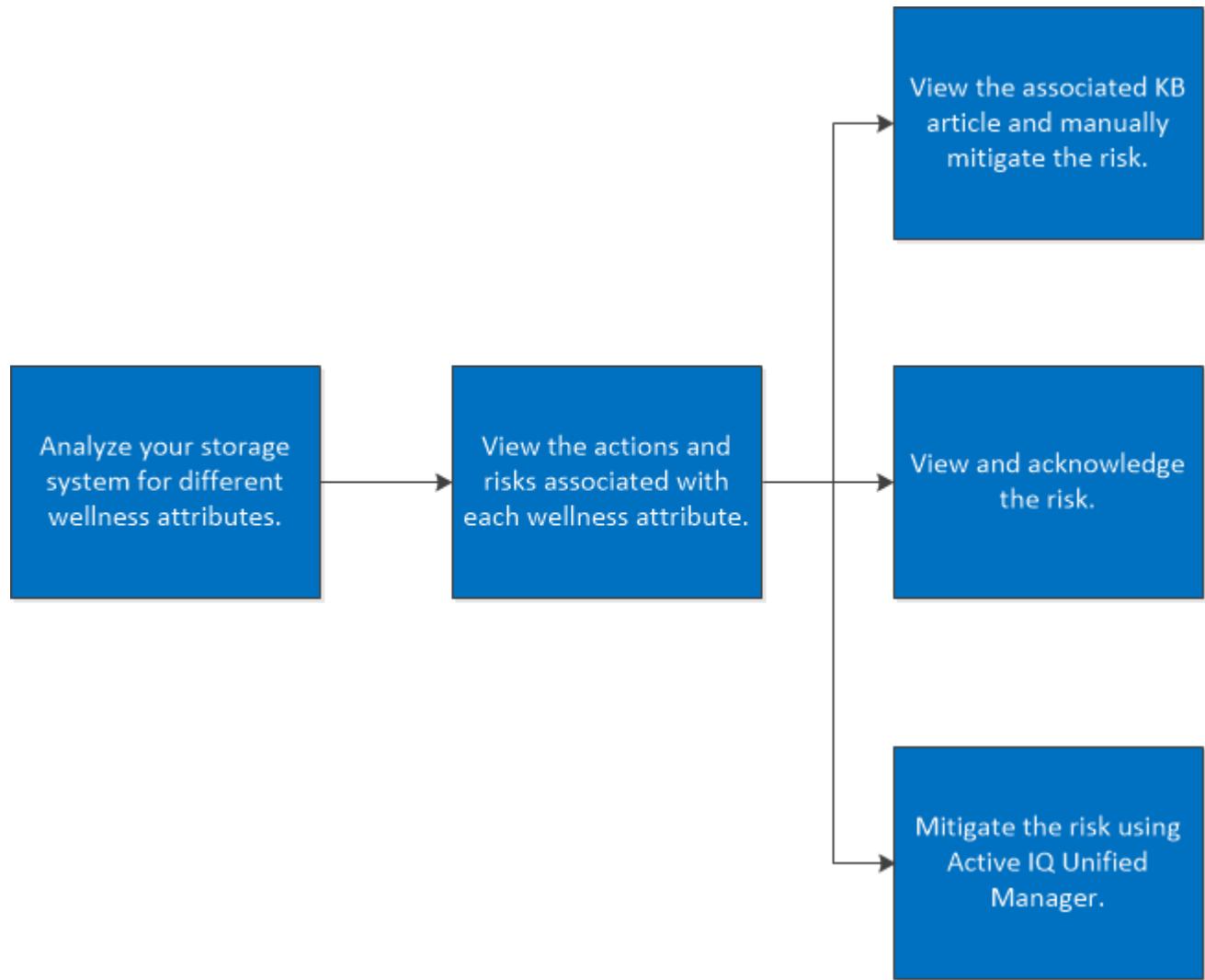
Table of Contents

Analyze wellness attributes	1
Learn about wellness widget in Digital Advisor	1
View storage system risks in Digital Advisor and take corrective actions	2
Detect security risks with Digital Advisor and take corrective actions	3
Protect storage systems managed by Digital Advisor from ransomware risks	4
Analyze wellness attributes in Digital Advisor and acknowledge risks	4
View your storage system risk history in Digital Advisor	5
View risks for actions in Digital Advisor and mitigate using Unified Manager or Ansible Playbook	5
Use Digital Advisor to fix critical risks identified in the Availability and Protection widget	7
Subscribe to storage system health notifications from Digital Advisor	8
Identify software and hardware renewals for your storage system from Digital Advisor	9
View the health of clusters and nodes using ClusterViewer widget in Digital Advisor	9

Analyze wellness attributes

Learn about wellness widget in Digital Advisor

Wellness widget provides detailed information about your storage system. It provides information about different attributes of your storage system, such as performance and efficiency, capacity, configuration settings, security vulnerabilities, renewals, and others.

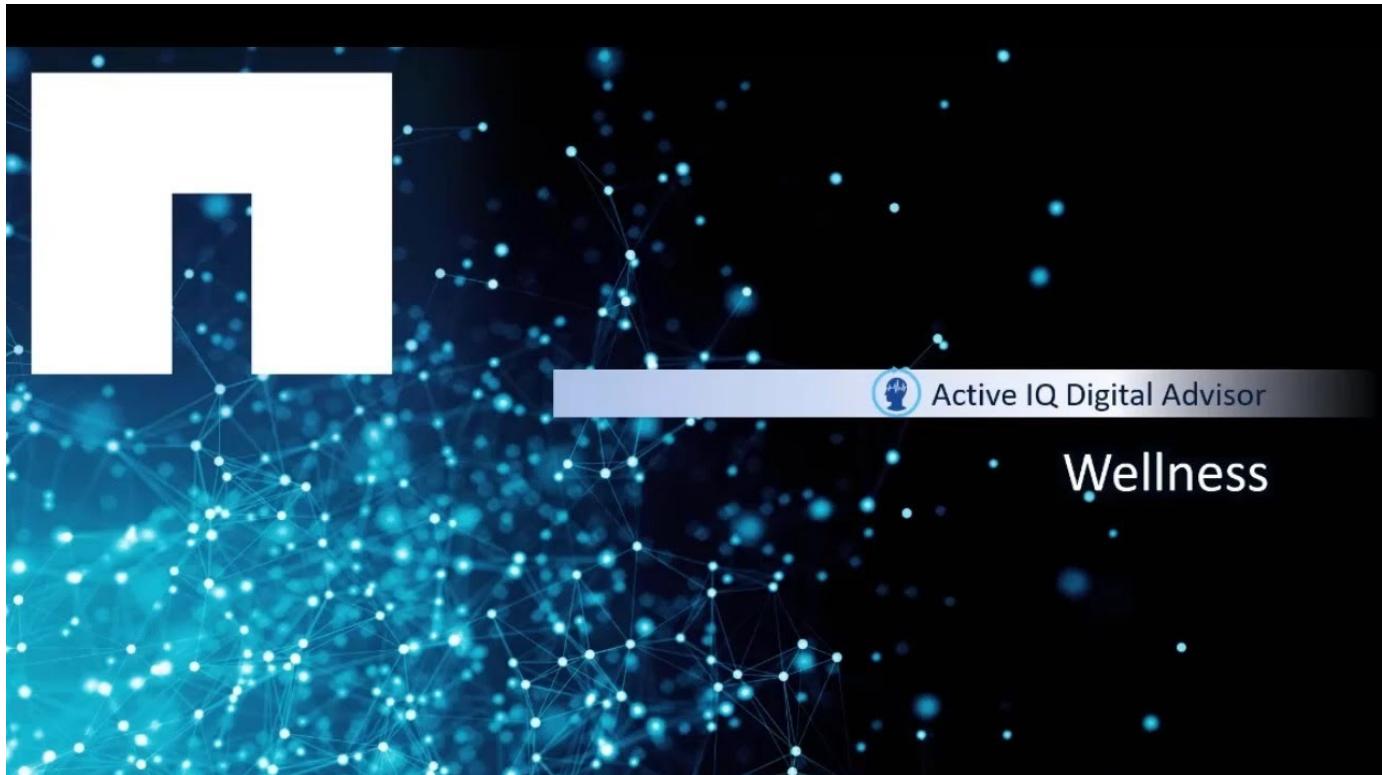


The wellness widget also provides information about the risks and the actions that should be taken to mitigate the risk for each wellness attribute. The following are the types of risks and the associated consequence for each risk:

Risk Type	Consequence
Critical	Data loss, data corruption, cluster data outage, personal safety issue, or potential legal compliance issue.
High	Short-term loss of data access or prolonged loss of node redundancy.
Medium	Performance degradation or short-term loss of node redundancy.

Risk Type	Consequence
Low	Low impact scenarios
Best Practice	Deviations from documented best practices

You can view the following video to understand the importance of the wellness attributes:



View storage system risks in Digital Advisor and take corrective actions

You can analyze the wellness attributes of your storage system by viewing the actions and risks associated with them. You should view the associated corrective actions and manually mitigate the risk.

Steps

1. Click the **Wellness** widget on the dashboard or click **View All Actions** to view the list of all the actions and risks.
2. View the **Actions** and **Risks** associated with the wellness attribute.
3. Click **Actions** to view the risks associated with the actions, click **Risks** to view all the risks, or click **Affected Systems** to view the systems that require attention.
4. Click the risk name to view information about the risk.
5. Click the associated corrective actions and follow the information to resolve the risk.

The steps to mitigate the risks are same for all wellness attributes. You can view the following video to monitor and fix security related issues:



Detect security risks with Digital Advisor and take corrective actions

The NetApp security site is the source of truth for NetApp Product Security: [NetApp Product Security](#)

Digital Advisor utilizes telemetry data and published product security advisories to detect security issues for covered* and support-entitled products. Product telemetry data must be transmitted to NetApp via AutoSupport to allow Digital Advisor to detect risks.

For additional NetApp product security information, including products not covered by Digital Advisor, visit [NetApp Product Security](#)

*Covered products: ONTAP 9 (on-prem and cloud), SANtricity OS Controller Software, NetApp SolidFire (Element Software), StorageGRID, Active IQ Unified Manager, ONTAP Tools for VMware (OTV)

Steps

1. Log in to Digital Advisor.
2. Click **Actions** in the **Security & Ransomware Defense** widget.



3. Clear the **Ransomware Defense** checkbox.
4. For the high-impact security risks, follow the recommended action that is to upgrade the operating system.
5. Click the **Unique Risks** tab, and then click the link in the **Corrective Action** column.

The risk is fixed in ONTAP 9.7P8 and later.

Advisory ID: NTAP-20200814-0005 Version: 6.0 Last updated: 12/03/2020 Status: Interim. CVEs: CVE-2020-9490, CVE-2020-11984, CVE-2020-11993

Overview Affected Products Remediation Revision History

Software Versions and Fixes

NetApp's currently available patches are listed below.

Product	First Fixed in Release
Clustered Data ONTAP	https://mysupport.netapp.com/site/products/all/details/ontap9/downloads-tab/download/62286/9.5P15 https://mysupport.netapp.com/site/products/all/details/ontap9/downloads-tab/download/62286/9.6P11 https://mysupport.netapp.com/site/products/all/details/ontap9/downloads-tab/download/62286/9.7P8

6. The most important step is to plan OS upgrade in the **Upgrade Advisor** in Digital Advisor.

Protect storage systems managed by Digital Advisor from ransomware risks

When you log in to the Digital Advisor, you can view the **Actions** highlighted on the **Security & Ransomware Defense** widget, which shows the risk counts.

You can view the Snapshot creation, retention, and ONTAP FPolicy risks, and then take actions to fix them.

Steps

1. Log in to Digital Advisor.
2. Click **Actions** on the **Security & Ransomware Defense** widget.
3. Clear the **Security Vulnerabilities** checkbox.
4. For the risks that are displayed, check the impact level and follow the recommended actions.
5. Click the Unique Risks tab and link in the **Corrective Action** column.
6. Click the **Affected Systems** tab to view systems with risks.
7. Follow remediation actions that are recommended to protect the systems.

Analyze wellness attributes in Digital Advisor and acknowledge risks

You can analyze the wellness attributes of your storage system by viewing the actions and risks associated with them. You should view the corrective actions and manually mitigate the risk.

Steps

1. Click the wellness attribute widget on the dashboard or click **View All Actions** to view the list of all the actions and risks.
2. View the **Actions** and **Risks** associated with the wellness attribute.
3. Click **Actions** to view the risks associated with the actions, click **Risks** to view all the risks, or click **Affected Systems** to view the systems that require attention.
4. Click the risk to view the risk summary.
5. Click **Ack** to acknowledge the risk.

The detailed risk summary information is provided along with corrective actions that should be manually performed to mitigate the risk.

6. If you do not want to or are unable to mitigate the risk at this time, provide the values for the fields and click **Acknowledge**.

The risk will be added to acknowledged risks.



If you no longer want a risk to be acknowledged, you can disregard the risk by clicking **Un-Ack** and following the same steps.

View your storage system risk history in Digital Advisor

You can view storage system risks occurring in the past three months, so that you can learn how they are faring overtime.

These risks are classified under four types of risks— **Unresolved**, **New**, **Resolved**, and **Acknowledged**. They are represented by different colors. The summary of these risks is represented through a **Risk History** graph.

Steps

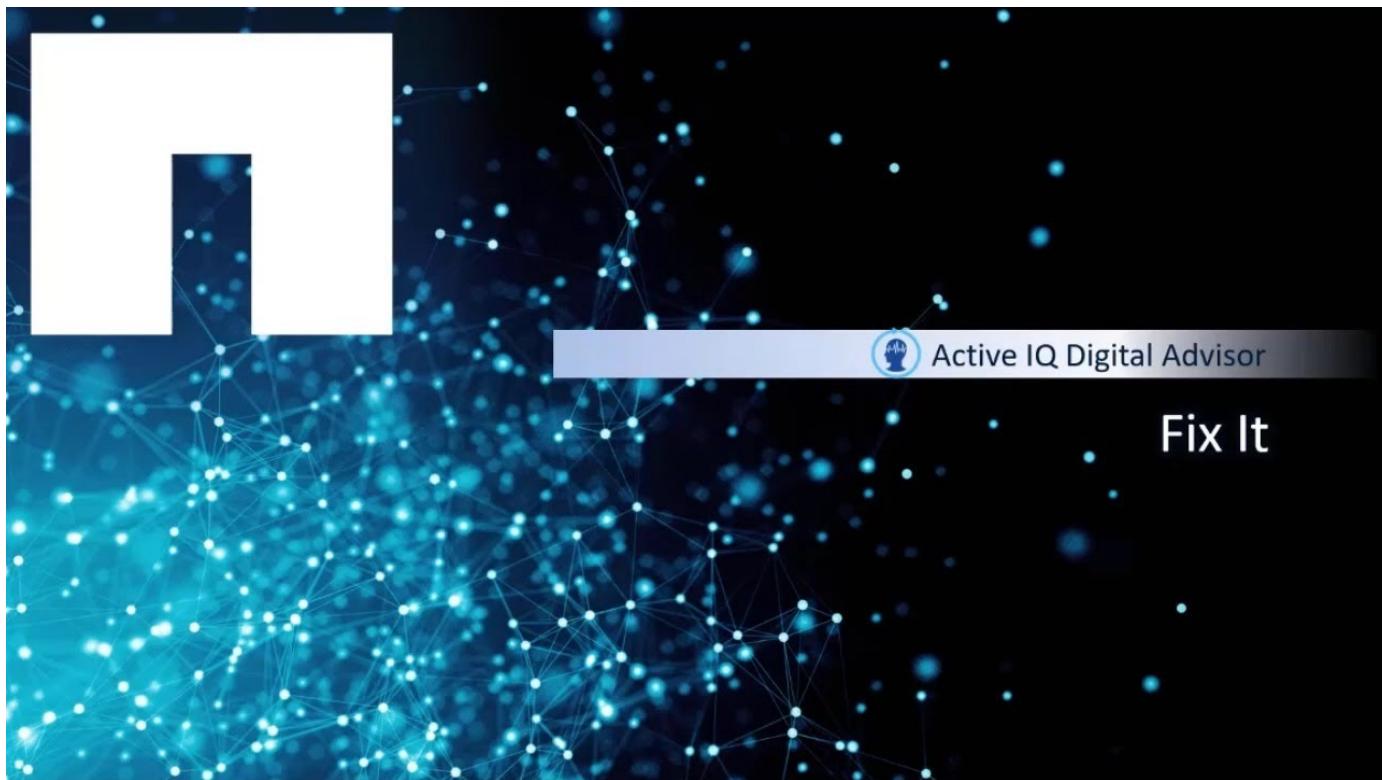
1. On the dashboard, in the **Wellness** pane, click **View All Actions**.
2. Click **Wellness History**.
3. In the **Risk History** graph, click the category for which you want to view the risk history.

When you hover over the colored bars, they display information on the number of risks in each category. Upon clicking the respective risk category, the information gets displayed in the **Risk Information** table.

You can also download risk summary in an Excel sheet.

View risks for actions in Digital Advisor and mitigate using Unified Manager or Ansible Playbook

You can analyze your storage system by viewing the actions and risks, and mitigate them using Active IQ Unified Manager or Ansible Playbook.



Steps

1. Click **View All Actions** on the dashboard.
2. Click **Actions** to view the risks associated with the actions, click **Risks** to view all the risks, or click **Affected Systems** to view the systems that require attention.

If the risk can be mitigated using Active IQ Unified Manager, the  icon is highlighted and if the risk can be mitigated using Ansible Playbook, the  icon is highlighted.

To mitigate the risk using Unified Manager	To mitigate the risk using Ansible Playbook
<ol style="list-style-type: none">1. Click the  icon.2. Click Fix It to launch Active IQ Unified Manager.3. Click Install to install Active IQ Unified Manager 9.7 or later to use the Fix It option.4. Click Upgrade to upgrade to Active IQ Unified Manager 9.7 or later to use the Fix It option.	<ol style="list-style-type: none">1. Click the  icon.2. Click Download to download the AFF and FAS firmware Ansible Automation package.



A SupportEdge Advisor or SupportEdge Expert contract is required to use the **Fix It** option and the Ansible Playbook features.

Use Digital Advisor to fix critical risks identified in the Availability and Protection widget

When you log in to the Digital Advisor and notice the red badge on the **Availability and Protection** widget, you can take actions to fix critical risks. Without the firmware fix, these drives are vulnerable to become inoperable after a certain number of hours of being powered on. Fixing this would avoid both the downtime and possible data loss.

Steps

1. Log in to the Digital Advisor.
2. Click **Actions** in the **Availability & Protection** widget.



For the high-impact security risks, follow the recommended action that is to update disk firmware.

3. Click the **Risk Name** link for viewing risk summary.

A screenshot of the 'Risk Summary' page. The page has a header 'Risk Summary' and a close button 'X'. It contains the following information:

- Impact:** High
- Mitigation:** Potentially Non-disruptive
- Public:** Yes
- Category:** FAS Hardware
- Internal Info:** Signature: 5608
- Corrective Action:** KB ID: 5U448

Risk:
CRITICAL - NetApp has identified certain SSD (Solid State Drive) models that have a higher failure rate compared to other models shipped by NetApp.

Potential Impact:
The drive model(s) identified will fail after 70,000 power-on hours (~8 years of use), which could lead to data loss or outage if multiple drives are simultaneously affected.

Details:
This storage system has 120 model X447_PHM2800MCTD drives installed that are not running the latest firmware.

4. Click the **Unique Risks** tab, and then click the link in the **Corrective Action** column.

Fix It	Risk Name	Mitigation ↑	Corrective Action	Systems	Impact ↑
	CRITICAL - NetApp has identified certain SSD (Solid State Drive) models that have a higher failure rate compared to other models shipped by NetApp.	Potentially Non-disruptive	KB ID: 5U448	4	High

Digital Advisor generates custom Ansible scripts or playbooks to update the required disk firmware, including the disk firmware files.

5. Click the **Ansible “A”** icon to generate and download the scripts.

A Update AFF and FAS Firmware

[Quick Start Guide](#)

Risk Name:

CRITICAL - NetApp has identified certain SSD (Solid State Drive) models that have a higher failure rate compared to other models shipped by NetApp.

Disk Firmware Download Summary (2 Files)

- Ansible Playbook and Inventory - **1 File**
- Disk Firmware - **1 File**

Suggestion:

You should be logged in to [NetApp Support Site](#) to download the files.

[Download](#)

Subscribe to storage system health notifications from Digital Advisor

You can subscribe to the wellness review email to receive a monthly email that summarizes wellness status, storage systems that are nearing their renewal dates, storage systems that require an upgrade for the NetApp products in your installed base. You will receive a wellness review email so that you can view a monthly summary and take action for your storage systems.

You also have options to view, edit, share, and delete your subscriptions. At any time, if you decide to not receive the email, you can unsubscribe from getting email as well.

After the subscription is enabled, you should select a start date when adding a subscription. The monthly email summary provides a view of outstanding wellness, renewal, upgrade, and health check actions. You can confirm the email address and the email is sent to the specified email address. You also have the option to delete subscriptions.



This feature is available only through NetApp SupportEdge Advisor and SupportEdge Expert service offerings.

Steps

1. From the left pane, click **Wellness Review**.
2. Click **Add Subscription**.
3. Provide the required information in the **Name the Subscription**, **Choose Category**, **Search Customer**, and **Email** fields in the **Add New Subscription** dialog box.
4. Click **Subscribe**.

Upon successful subscription, you will receive a **Subscription was added** message.

Identify software and hardware renewals for your storage system from Digital Advisor

You can proactively identify the software and hardware for your storage system that have expired or are near expiration in the next 6 months, and send a request to renew the hardware and software.

Steps

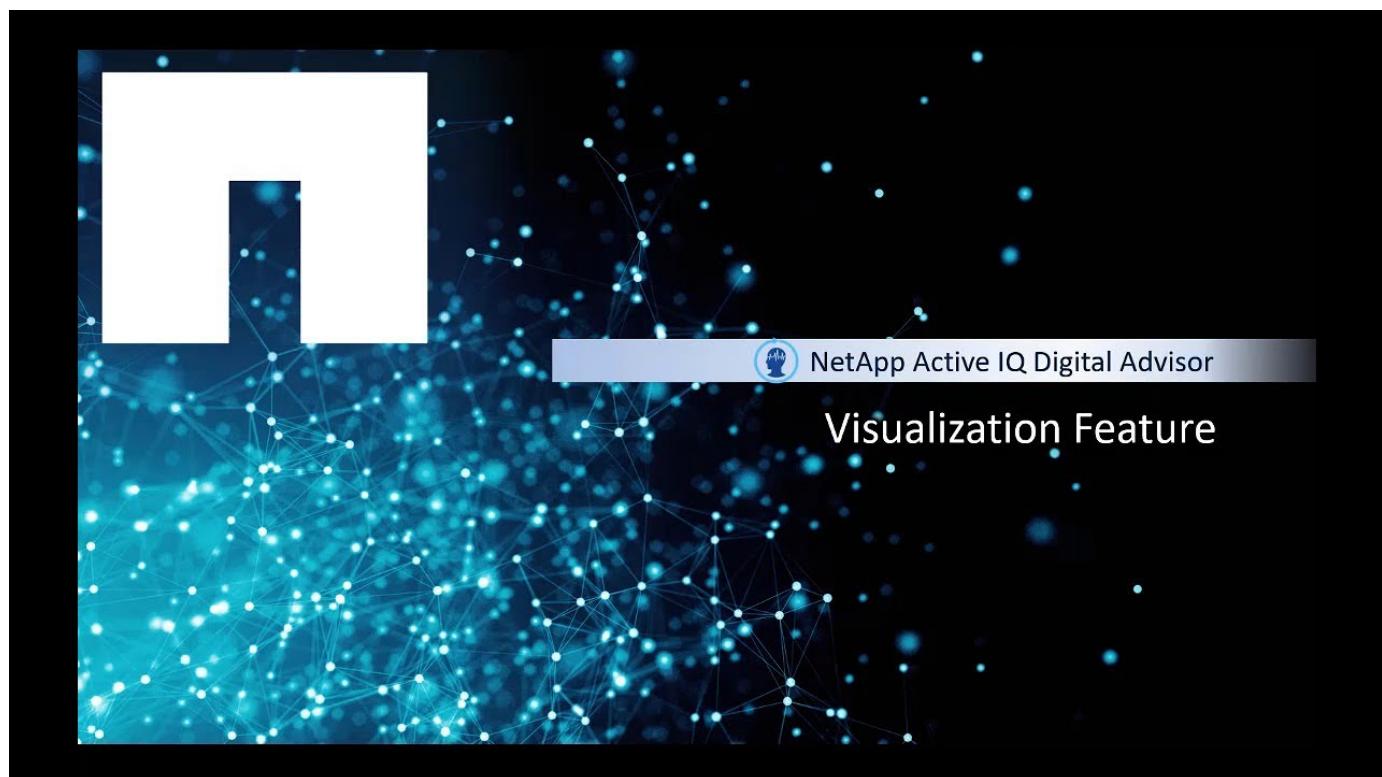
1. Click **Renewals** from the **Planning** widget.
2. Select the storage systems that you want to renew and click **Renew**.
3. Optionally, provide additional comments.
4. Click **Send**.

View the health of clusters and nodes using ClusterViewer widget in Digital Advisor

You can analyze the wellness of your clusters and nodes using ClusterViewer, a one-stop source for information on the physical and logical configuration of your clusters and nodes.

ClusterViewer provides information, such as stack diagrams of your nodes, storage usage and efficiency, headroom in hardware capacity, and so on, that helps you take informed decisions to improve the wellness of your clusters and nodes.

You can view visualizations or graphical representations of the physical configuration of your nodes at cable, stack, and RAID Disk levels. You can also download the visualizations in SVG format.



Steps

1. In the **Inventory** widget, select the cluster or node (host) that you want.
2. At the cluster or node level, click **ClusterViewer** next to the **Configuration** widget.
3. Click the **Visualization** tab to view a graphical representation of the cluster.

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—with 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.