Fix or manage ONTAP issues directly from Unified Manager

Active IQ Unified Manager

NetApp
September 26, 2026

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

Table of Contents

Fix or manage ONTAP issues directly from Unified Manager . . . 1
Manage ONTAP issues or features directly from Active IQ Unified Manager . . . 1
Learn about the Fix It and Fix All button options in Active IQ Unified Manager . . . 1
View the status of management actions to fix in Active IQ Unified Manager . . . 2
Learn about ONTAP issues that Active IQ Unified Manager can fix . . . 3
Override management actions with scripts in Active IQ Unified Manager . . . 7

Fix or manage ONTAP issues directly from Unified Manager

Manage ONTAP issues or features directly from Active IQ Unified Manager

You can fix certain ONTAP issues or manage certain ONTAP features directly from the Unified Manager user interface, instead of having to use ONTAP System Manager or the ONTAP CLI. The “Management Actions” option provides fixes to a number of ONTAP issues that have triggered Unified Manager events.

You can fix issues directly from the Management Actions page by selecting the **Management Actions** option on the left navigation pane. Management Actions are also available from the Management Actions panel on the Dashboard, Event details page, and Workload Analysis selection on the left-navigation menu.

There are certain issues that Unified Manager can diagnose thoroughly and provide a single resolution. For certain ONTAP features, such as anti-ransomware monitoring, Unified Manager performs internal checks and recommends specific actions. When available, those resolutions are displayed in Management Actions with a **Fix It** button. Click the **Fix It** button to fix the issue. You must have the Application Administrator or Storage Administrator role.

Unified Manager sends ONTAP commands to the cluster to make the requested fix. When the fix is complete the event is obsoleted.

Some management actions enable you to fix the same issue on multiple storage objects using the **Fix All** button. For example, there may be 5 volumes that have the "Volume Space Full" event that could be resolved by clicking the **Fix All** management action for "Enable volume autogrow". One click enables you to fix this issue on 5 volumes.

For information about the ONTAP issues and features that you can manage by using automatic remediation, see What issues can Unified Manager fix.

Learn about the Fix It and Fix All button options in Active IQ Unified Manager

The Management Actions page provides you with the **Fix It** or **Fix All** button to fix issues that Unified Manager has been notified about through an event.

We recommend that you click the buttons to fix an issue, as required. However, if you are not sure that you want to resolve the issue as recommended by Unified Manager, you can perform the following actions:

What do you want to do?	Action
Have Unified Manager fix the issue on all identified objects.	Click the **Fix All** button.
Do not fix the issue for any of the identified objects at this time and hide this management action until the event is raised again.	Click the down arrow and click **Dismiss All**.

What do you want to do?	Action
Fix the issue on only some of the identified objects.	Click the name of the management action to expand the list and show all individual **Fix It** actions.Then follow the steps for fixing or dismissing individual management actions.

What do you want to do?	Action
Have Unified Manager fix the issue.	Click the **Fix It** button.
Do not fix the issue at this time and hide this management action until the event is raised again.	Click the down arrow and click **Dismiss**.
Display the details for this event so you can better understand the issue.	• Click the **Fix It** button and review the fix that will be applied in the resulting dialog box. • Click the down arrow and click **View Event Detail** to display the Event details page. Then click **Fix It** from either of these resulting pages if you want to fix the issue.
Display the details for this storage object so you can better understand the issue.	Click the name of the storage object to display details in either the Performance Explorer or Health Details page.

In some cases the fix is reflected in the next 15 minute configuration poll. In other cases it can take up to many hours for the configuration change to be verified and for the event to be obsoleted.

To see the list of completed or in progress management actions, click the filter icon and select **Completed** or **In Progress**.

Fix All operations run in a serial fashion, so when you view the **In Progress** panel some objects will have the Status **In Progress** whereas others will have the Status **Scheduled**; meaning they are still waiting to be implemented.

View the status of management actions to fix in Active IQ Unified Manager

You can view the status of all management actions that you have chosen to fix in the Management Actions page. Most actions are shown as **Completed** fairly quickly after Unified Manager sends the ONTAP command to the cluster. However, some actions, such as moving a volume, can take longer.

There are three filters available on the Management Actions page:

- **Completed** shows both management actions that completed successfully and those that have failed. **Failed** actions provide a reason for the failure so that you can address the issue manually.
- **In Progress** shows both those management actions that are being implemented, and those that are scheduled to be implemented.
- **Recommended** shows all the management actions that are currently active for all monitored clusters.

Steps

1. Click **Management Actions** on the left navigation pane. Alternately, click ⋮ at the top of the **Management Actions** panel on the **Dashboard** and select the View you want to see.

   The Management Actions page is displayed.

2. You can click the caret icon next to the management action in the **Description** field to see details about the issue and the command that is being used to fix the issue.
3. To view any actions that **failed**, sort on the **Status** column in the **Completed** View. You can use the **Filter** tool for this same purpose.
4. If you want to view more information about a Failed management action, or if you decide that you want to fix a Recommended management action, you can click **View Event Detail** from the expanded area after you click the caret icon next to the management action. A **Fix It** button is available from that page.

Learn about ONTAP issues that Active IQ Unified Manager can fix

By using the automatic remediation feature of Active IQ Unified Manager, you can choose to resolve certain ONTAP issues or manage certain ONTAP features, such as anti-ransomware monitoring, effectively through Unified Manager.

This table describes these ONTAP issues or features that you can manage directly through the **Fix It** or **Fix All** button on the Unified Manager web UI.

Event Name and Description	Management Action	"Fix It" Operation
Volume Space Full The volume is almost out of space and it has breached the capacity full threshold. This threshold is set by default to 90% of the volume size.	Enable volume autogrow	Unified Manager determines that volume autogrow is not configured for this volume, so it enables this feature so the volume will grow in capacity when needed.
Inodes Full This volume has run out of inodes and cannot accept any new files.	Increase number of inodes on volume	Increases the number of inodes on the volume by 2 percent.
Storage Tier Policy Mismatch Detected The volume has lots of inactive data and the current tiering policy is set to "snapshot-only" or "none".	Enable automatic cloud tiering	Since the volume already resides on a FabricPool, it changes the tiering policy to "auto" so that inactive data is moved to the lower cost cloud tier.
Storage Tier Mismatch Detected The volume has lots of inactive data, but it does not reside on a cloud-enabled storage tier (FabricPool).	Change volumes' storage tier	Moves the volume to cloud-enabled storage tier and sets the tiering policy to "auto" to move inactive data to the cloud tier.

Event Name and Description	Management Action	"Fix It" Operation
Audit Log Disabled The audit log is not enabled for the storage VM	Enable audit logging for the storage VM	Enables audit logging on the storage VM. Note that the storage VM must already have either a local or remote audit log location configured.
Login Banner Disabled The login banner for the cluster should be enabled to increase security by making access restrictions clear.	Set login banner for the cluster	Sets the cluster login banner to “Access restricted to authorized users”.
Login Banner Disabled The login banner for the storage VM should be enabled to increase security by making access restrictions clear.	Set login banner for the storage VM	Sets the storage VM login banner to "Access restricted to authorized users".
SSH is Using Insecure Ciphers Ciphers with the suffix "-cbc" are considered insecure.	Remove insecure ciphers from the cluster	Removes the insecure ciphers — such as aes192-cbc and aes128-cbc — from the cluster.
SSH is Using Insecure Ciphers Ciphers with the suffix "-cbc" are considered insecure.	Remove insecure ciphers from the storage VM	Removes the insecure ciphers — such as aes192-cbc and aes128-cbc — from the storage VM.
AutoSupport HTTPS transport disabled The transport protocol used to send AutoSupport messages to technical support should be encrypted.	Set HTTPS as the transport protocol for AutoSupport messages	Sets HTTPS as the transport protocol for AutoSupport messages on the cluster.
Cluster Load Imbalance Threshold Breached Indicates that the load is imbalanced among the nodes in the cluster. This event is generated when the performance capacity used variance is more than 30% between nodes.	Balance cluster workloads	Unified Manager identifies the best volume to move from one node to the other to reduce the imbalance, and then moves the volume.

Event Name and Description	Management Action	"Fix It" Operation
Cluster Capacity Imbalance Threshold Breached Indicates that the capacity is imbalanced among the aggregates in the cluster. This event is generated when the used capacity variance is more than 70% between aggregates.	Balance cluster capacity	Unified Manager identifies the best volume to move from one aggregate to another to reduce the imbalance, and then moves the volume.
Performance Capacity Used Threshold Breached Indicates that the load on the node could become over utilized if you don’t reduce the utilization by one or more highly active workloads. This event is generated when the node performance capacity used value is more than 100% for more than 12 hours.	Limit high load on node	Unified Manager identifies the volume with the highest IOPS and it applies a QoS policy using the historical expected and peak IOPS levels to reduce the load on the node.
Dynamic Event Warning Threshold Breached Indicates that the node is already operating in an overloaded state due to the abnormally high load of some of the workloads.	Reduce overload in node	Unified Manager identifies the volume with the highest IOPS and it applies a QoS policy using the historical expected and peak IOPS levels to reduce the load on the node.
Takeover is not possible Failover is currently disabled, so access to the node’s resources during an outage or reboot would be lost until the node became available again.	Enable node failover	Unified Manager sends the appropriate command to enable failover on all nodes in the cluster.
Option Cf.takeover.on_panic is Configured OFF The nodeshell option "cf.takeover.on_panic" is set to **off**, which could cause an issue on HA-configured systems.	Enable takeover on panic	Unified Manager sends the appropriate command to the cluster to change this setting to **on**.
Disable nodeshell option snapmirror.enable The old nodeshell option "snapmirror.enable" is set to **on**, which could cause an issue during boot after upgrading to ONTAP 9.3 or greater.	Set snapmirror.enable option to off	Unified Manager sends the appropriate command to the cluster to change this setting to **off**.

Event Name and Description	Management Action	"Fix It" Operation
Telnet enabled Indicates a potential security issue because Telnet is insecure and passes data in an unencrypted manner.	Disable Telnet	Unified Manager sends the appropriate command to the cluster to disable Telnet.
Configure storage VM anti-ransomware learning Periodically checks for clusters with licenses for anti-ransomware monitoring. Validates whether a storage VM supports only NFS or SMB volumes in such a cluster.	Put storage VMs in a `learning` mode of anti-ransomware monitoring	Unified Manager sets anti-ransomware monitoring to `learning` state for the storage VMs through the cluster management console. Anti-ransomware monitoring on all the new volumes created on the storage VM are automatically moved to a learning mode. Through this enablement, ONTAP can learn the pattern of activity on the volumes and detect the anomalies due to potential malicious attacks.
Configure volume anti-ransomware learning Periodically checks for clusters with licenses for anti-ransomware monitoring. Validates whether a volume supports only NFS or SMB services in such a cluster.	Put volumes in `learning` mode of anti-ransomware monitoring	Unified Manager sets anti-ransomware monitoring to `learning` state for the volumes through the cluster management console. Through this enablement, ONTAP can learn the pattern of activity on the volumes and detect the anomalies due to potential malicious attacks.
Enable volume anti-ransomware Periodically checks for clusters with licenses for anti-ransomware monitoring. Detects whether the volumes are in the `learning` mode of anti-ransomware monitoring for more than 45 days, and determines the prospect of putting them in active mode.	Put volumes in `active` mode of anti-ransomware monitoring	Unified Manager sets anti-ransomware monitoring to `active` on the volumes through the cluster management console. Through this enablement, ONTAP can learn the pattern of activity on the volumes and detect the anomalies due to potential malicious attacks, and create alerts for data protection actions.
Disable volume anti-ransomware Periodically checks for clusters with licenses for anti-ransomware monitoring. Detects repetitious notifications during active anti-ransomware monitoring on the volumes (for example, multiple warnings of potential ransomware attacks are returned over 30 days).	Disable anti-ransomware monitoring on volumes	Unified Manager disables anti-ransomware monitoring on the volumes through the cluster management console.

Override management actions with scripts in Active IQ Unified Manager

You can create custom scripts and associate them to alerts to take specific actions for specific events, and not opt for the default management actions available for them on the Management Actions page or Unified Manager dashboard.

If you want to take specific actions for an event type and choose not to fix them as a part of the management action capability provided by Unified Manager, you can configure a custom script for the specific action. You can then associate the script with an alert for that event type and take care of such events individually. In this case, management actions are not generated for that specific event type on the Management Actions page or Unified Manager dashboard.

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.