



Well-architected dashboard in NetApp Console

Well-architected dashboard

NetApp
July 21, 2026

Table of Contents

- Get started 1
 - What’s new with the well-architected dashboard in NetApp Console 1
 - 20 July 2026 1
 - Learn about the well-architected dashboard in NetApp Console 1
 - How it works 1
 - Why it matters 2
 - Supported storage systems 2
 - Get started with NetApp Console to detect and fix system misconfigurations 2
 - Related information 2
- Supported products 3
 - Amazon FSx for NetApp ONTAP 3
 - Configuration analysis for Amazon FSx for NetApp ONTAP 3
 - Implement well-architected FSx for ONTAP file system configurations 6
 - Cloud Volumes ONTAP 8
 - Configuration analysis for Cloud Volumes ONTAP 8
 - Implement well-architected Cloud Volumes ONTAP system configurations 10
- Build your own rules 12
 - Learn about custom rules 12
 - Overview 12
 - How custom rules work 12
 - Before you begin 12
 - Limitations 12
 - Rule definition model 13
 - Rule lifecycle 13
 - Custom rule examples 13
 - What to do next 14
 - Create a custom rule 14
 - Create a rule 14
 - Review the AI interpretation 15
 - Test the rule 15
 - Save or schedule the rule 16
 - Troubleshooting 16
 - What to do next 16
- Manage custom rules 16
 - View the Rules catalog 17
 - View rule results 17
 - Pause a rule 17
 - Delete a custom rule 17
 - Run a quick test 17
 - Understand execution status 18
 - What to do next 18
- Legal notices 19
 - Copyright 19

Trademarks	19
Patents	19
Privacy policy	19
Open source	19

Get started

What's new with the well-architected dashboard in NetApp Console

Learn what's new with the well-architected dashboard in NetApp Console.

20 July 2026

Introducing the well-architected dashboard in NetApp Console

The well-architected dashboard in NetApp Console provides a single view of your storage systems and configurations across accounts and regions. The dashboard provides insights and recommendations to help you achieve operational excellence. You can view the well-architected status of your configurations, configuration issues organized by the pillars of the well-architected framework for the storage type you use, and a list of configuration issues and recommendations.

Learn more about the [well-architected dashboard](#).

The well-architected dashboard in the Console is available for the following storage systems:

- [Amazon FSx for NetApp ONTAP](#)
- [Cloud Volumes ONTAP in Microsoft Azure](#)

Build your own custom rules

Write custom rules in plain language to make sure your systems follow your organization's standards and NetApp best practices. Test the rules with a dry run, then schedule them to run across your environments.

[Learn more about custom rules](#)

Learn about the well-architected dashboard in NetApp Console

The well-architected dashboard in NetApp Console helps you maintain and operate reliable, secure, efficient, and cost-effective configurations that align with the well-architected frameworks for the storage type you use. The dashboard provides a unified view across accounts and regions, helps teams identify and prioritize risks, and supports custom rules for specific requirements. Automatic daily scans of your storage system configurations provide insights and recommendations to help you optimize your storage environments.

How it works

The well-architected dashboard analyzes your configurations daily. The analysis provides well-architected status, insights, and recommendations.

After the daily analysis completes, configurations appear as "optimized" or "not optimized" in the well-architected dashboard. You'll find the total optimization score, configuration issues by category, and a list of

configuration issues and recommendations. You can review the recommendations for configuration issues. Some issues can be fixed automatically by the well-architected dashboard, while others require manual intervention. In this case, the well-architected dashboard provides detailed instructions to help you implement the recommended changes.

You can dismiss the analysis of configurations that do not apply to your environments. This avoids unnecessary alerts and inaccurate optimization results. When you dismiss a specific configuration analysis, the well-architected dashboard does not include the configuration in the total optimization score.

Why it matters

The well-architected dashboard in NetApp Console applies best practices to large storage, database, and VMware environments by combining ongoing assessment with recommendation insights and remediation. Automated remediation applied in the well-architected dashboard reduces human error, ensures uniform management, and preserves performance and reliability across your system infrastructures.

Supported storage systems

The well-architected dashboard in the Console supports the following storage systems:

- Amazon FSx for NetApp ONTAP
- Cloud Volumes ONTAP in Microsoft Azure

Get started with NetApp Console to detect and fix system misconfigurations

To get started with NetApp Console, sign up, add credentials, and establish connectivity to manage your resources and optimize system configurations.

[Get started workflow for NetApp Console \(SaaS application\)](#)

Related information

- [Implement well-architected FSx for ONTAP file systems](#)
- [Implement well-architected Cloud Volumes ONTAP systems](#)

Supported products

Amazon FSx for NetApp ONTAP

Configuration analysis for Amazon FSx for NetApp ONTAP

The well-architected dashboard in NetApp Console analyzes storage system configurations regularly to determine if any there are any configuration issues with your Amazon FSx for NetApp ONTAP file systems. When issues are found, the dashboard shows you what the issues are and explains what needs to change to ensure your storage systems achieve peak performance, cost efficiency, and compliance with best practices.

Key capabilities include:

- Daily configuration analysis
- Automatic best practice validations for NetApp ONTAP storage systems and partner storage providers
- Proactive observability
- Insights to action

Analysis requirements

For a complete file system analysis, you must do the following:

- [Deploy a NetApp Console agent](#) or [associate a link](#) to set up connectivity between the file system and NetApp Console.
- Grant *view*, *planning*, and *analysis* permissions in your AWS account.

[Learn how to grant permissions to an AWS account](#)

Best practices and recommendations for storage workloads

The well-architected dashboard assesses storage configurations against ONTAP best practices and the AWS Well-Architected Framework. The assessment also recommends improvements and fixes.

The well-architected analysis categorizes configurations in the following pillars of the framework: *reliability*, *security*, *operational excellence*, *cost optimization*, and *performance efficiency*.

Reliability

Reliability ensures that workloads perform their intended functions correctly and consistently, even when there are disruptions.

- **Schedule volume backups**

Backing up your volumes helps support data retention and compliance needs. Use volume backups to set up automated backups and retention for your data.

- **Schedule local snapshots**

Schedule local snapshots for efficient backup and quick restores. Snapshots are instant, point-in-time images of your volumes.

- **Cross-region replication**

Cross-region replication ensures that your data is replicated to another AWS region, providing enhanced data durability and availability. Set up cross-region replication to support disaster recovery and compliance.

- **Set up data replication**

To extend data reliability, replicate data to an FSx for ONTAP file system in the same region or in another region. Set up data replication to support migration, disaster recovery, and long-term retention across file systems.

- **Increase SSD capacity threshold**

The SSD storage tier capacity should not exceed 80% utilization. This might impact data reads and writes to your capacity pool storage tier and impact the throughput capacity of your file system. When capacity runs out, data volumes become read-only. Services trying to write new data also fail.

- **Match labels to ensure data reliability**

The snapshot policy labels of the source volume and the replication policy labels must match to ensure data reliability.

- **Increase file capacity threshold**

The file capacity threshold should be raised to avoid hitting the volume capacity limit. Low file capacity (inodes) prevents writing additional data to the volume. Workload Factory recommends maintaining file capacity utilization below 80% to allow new file creation.

Security

Security emphasizes protecting data, systems, and assets through risk assessments and mitigation strategies.

- **Enable ARP/AI**

NetApp Autonomous Ransomware Protection with AI (ARP/AI) helps protect your volumes from ransomware threats. Workload Factory recommends enabling ARP/AI for all volumes.

- **Unauthorized access to volumes**

Volumes serving application data using iSCSI should not allow NAS access at the same time. Workload Factory recommends restricting iSCSI volumes from using any other protocol.

Operational excellence

Operational excellence focuses on delivering the most optimal architecture and business value.

- **Enable automatic capacity management**

Automatic capacity management should be enabled to regularly ensure that the SSD tier doesn't exceed the threshold.

- **Volume capacity utilization threshold**

Workload Factory recommends that volume capacity doesn't exceed 80% utilization. This might impact data reads and writes to your application. Volume capacity increases can be manual or automatic using the volume autogrow feature.

- **Volume utilization nearing full**

When a volume is nearing full capacity, Workload Factory recommends taking action to increase the volume capacity to avoid potential application disruptions.

- **Cache relationship write mode**

For optimal performance, Workload Factory recommends the cache relationship write mode that best suits your workload. Write-around mode provides better performance for read-heavy workloads with small files, whereas write-back mode provides better performance for write-heavy workloads with large files.

- **Optimize cache volume size**

Workload Factory recommends enabling volume autosize and scrubbing on cache volumes to maintain optimal size and focus the cache on hot data for peak efficiency.

- **Storage VM logical reporting**

Workload Factory recommends that the default reporting setting is set to logical for a storage VM to provide better visibility into storage usage at the volume level.

Cost optimization

Cost optimization helps you get the most value for your business while keeping costs low.

- **Optimize TCO by tiering cold data**

Enable cold data tiering to reduce SSD storage tier utilization. Workload Factory recommends applying a tiering policy to every volume. FSx for ONTAP continuously scans the data for cold data and moves it to the capacity pool tier without disruption.

- **Enable storage efficiencies**

Enable storage efficiencies — compaction, compression, and deduplication — to optimize storage utilization and reduce the SSD tier cost.

- **Unnecessary snapshot and backup deletion**

Delete snapshots and backups that are no longer needed to reduce costs.

- **Inactive block devices**

After a block device isn't used for seven days, Workload Factory recommends archiving block device data or deleting the unused block device to reduce costs.

- **Underutilized SSD capacity**

An underutilized SSD capacity tier adds unnecessary costs. Workload Factory recommends reducing the SSD tier capacity while maintaining a 20% free space buffer. A decrease operation takes several hours to several days, and other file system operations are unsupported during this time.

- **Inactive NAS volumes**

The configuration analysis identifies NAS volumes that are not actively used and recommends deleting or archiving the volumes to reduce costs.

What's next

[Implement well-architected FSx for ONTAP file system configurations](#)

Implement well-architected FSx for ONTAP file system configurations

Using configuration analysis insights and recommendations, leverage NetApp to implement best practices for your FSx for ONTAP file systems. You can easily review the well-architected status, learn about issues with your configurations, take action to improve the architecture of any systems that aren't optimized for reliability, security, efficiency, performance, and cost.

You can also dismiss the analysis of specific storage configurations that don't apply to your storage environment to avoid unnecessary alerts and inaccurate optimization results.

[Learn about the configuration analysis and well-architected status.](#)

About this task

The well-architected dashboard analyzes Amazon FSx for NetApp ONTAP file system deployment configurations daily. The daily analysis provides the well-architected status, insights, and recommendations. You can automatically fix configuration issues to meet best practices.

Link or Console agent connectivity allows the well-architected dashboard in the NetApp Console to complete a comprehensive scan of your file systems for issues with performance, data protection, and configurations. This ensures that you receive accurate insights and recommendations for optimizing your FSx for ONTAP file systems.

Storage configuration requirements vary. You can dismiss the analysis of specific configurations that don't apply to your storage environment. This helps you avoid unnecessary alerts and inaccurate optimization results.

Before you begin

- You must [grant *operations and remediation* permissions](#) in your AWS account.
- [Install a Console agent](#) or [Connect to an FSx for ONTAP file system using a link](#) for the most comprehensive analysis of your file system resources.

Fix a configuration issue

You can fix configuration issues for an FSx for ONTAP file system or for selected volumes in a file system. You can select one or more configurations to fix.

Fixing configuration issues can cause instance downtimes or service interruptions. Review each recommendation carefully before fixing a configuration issue.

Steps

1. Log in to the [NetApp Console](#).

2. From the NetApp Console menu, select **Workloads** and then **Well-architected**.
3. From the Well-architected dashboard, select **View** for any configuration.

Make sure you review the recommendation carefully. The recommendation explains best practices and potential pitfalls of unoptimized configurations.

4. Select to **Fix**.

When **View and fix** is an option, select the impacted volumes to fix.

5. Review the summary and action items in the dialog to learn what happens if you fix the issue. Some operations can cause instance downtimes or service interruptions.
6. Select **Continue** to fix the configuration issue.

Result

Workload Factory starts the process to fix the issue. Select the account settings menu and then select **Tracker** to view the status of the operation.

Dismiss a configuration analysis

Stop a configuration analysis for an FSx for ONTAP file system or for selected volumes. You can restart the analysis when needed.

Dismiss a configuration analysis for a file system

Steps

1. Log in to the [NetApp Console](#).
2. From the NetApp Console menu, select **Workloads** and then **Well-architected**.
3. Under Configurations, identify the configuration that doesn't apply to your environment and then select **Dismiss**.
4. In the Dismiss configuration dialog, select **Dismiss** to stop the configuration analysis.

Dismiss a configuration analysis for a volume

Steps

1. Log in to the [NetApp Console](#).
2. From the NetApp Console menu, select **Workloads** and then **Well-architected**.
3. Under Configurations, identify the configuration to dismiss for selected volumes and then select **View and fix**.
4. Identify the volumes to dismiss from the configuration analysis.
 - For one volume: select the actions menu and then select **Dismiss volume**.
 - For multiple volumes: select the volumes and then select **Dismiss** next to Bulk action.
5. Select **Dismiss** to stop the analysis for the configuration.
6. In the Dismiss volumes dialog, select **Dismiss** to confirm.

Result

The configuration analysis stops for the file system or selected volumes.

You can reactivate the analysis at any time.

Reactivate a dismissed configuration analysis

Reactivate a dismissed configuration analysis at any time. You can select one or more configurations to reactivate.

Reactivate a configuration analysis for a file system

Steps

1. Log in to the [NetApp Console](#).
2. From the NetApp Console menu, select **Workloads** and then **Well-architected**.
3. From the Well-architected dashboard, select **Dismissed configurations**.
4. Identify the configuration you want to reactivate and select **Reactivate**.

Reactivate a configuration analysis for a volume

Steps

1. Log in using one of the [console experiences](#).
2. Select the menu and then select **Storage**.
3. From the Storage menu, select **Well-architected**.
4. Select **Dismissed configurations**.
5. Identify the volume(s) to reactivate from the configuration analysis.
 - For one volume: select the actions menu and then select **Reactivate volume**.
 - For multiple volumes: select the volumes and then select **Reactivate** next to Bulk action.

Result

The configuration analysis reactivates. Workload Factory runs a new analysis daily.

Cloud Volumes ONTAP

Configuration analysis for Cloud Volumes ONTAP

The well-architected dashboard in NetApp Console analyzes storage system configurations regularly to determine if there are any configuration issues with your Cloud Volumes ONTAP systems. When issues are found, the dashboard shows you what the issues are and explains what needs to change to ensure your storage systems achieve peak performance, cost efficiency, and compliance with best practices.

Key capabilities include:

- Daily configuration analysis
- Automatic best practice validations for NetApp ONTAP storage systems and partner storage providers
- Proactive observability
- Insights to action

Analysis requirements

For a complete Cloud Volumes ONTAP system analysis, you must [deploy a NetApp Console agent](#) to set up connectivity between your systems and the NetApp Console.

Best practices and recommendations for Cloud Volumes ONTAP systems

The well-architected dashboard assesses storage configurations to provide an in-depth view of ONTAP configuration best practices and for compliance with the Azure Well-Architected Framework. The assessment also recommends improvements and fixes.

The well-architected analysis categorizes configurations in the following pillars of the framework: *reliability*, *security*, *operational excellence*, *cost optimization*, and *performance efficiency*.

Reliability

Reliability ensures that workloads perform their intended functions correctly and consistently, even during disruptions.

- **Schedule local snapshots**

Schedule local snapshots for efficient backup and quick restores. Snapshots are instant, point-in-time images of your volumes.

- **SSD capacity threshold**

The SSD storage tier capacity should not exceed 80% utilization on an ongoing basis. Exceeding this threshold can degrade throughput, make data volumes read-only, and cause write operations to fail.

Security

Security emphasizes protecting data, systems, and assets through risk assessments and mitigation strategies.

- **Autonomous Ransomware Protection with AI (ARP/AI)**

NetApp Autonomous Ransomware Protection with AI (ARP/AI) helps enhance cyber resiliency and protect your volumes from ransomware threats. We recommend enabling ARP/AI for all volumes.

Operational excellence

Operational excellence focuses on delivering the best architecture and business value.

- **Volume capacity utilization threshold**

NetApp recommends that volume capacity doesn't exceed 80% utilization on an ongoing basis. This might impact data reads and writes to your application. Volume capacity increases can be manual or automatic using the volume autogrow feature.

- **Cache relationship write mode**

For optimal performance, NetApp recommends the cache relationship write mode that best suits your workload. Write-around mode provides better performance for read-heavy workloads with small files, while write-back mode provides better performance for write-heavy workloads with large files.

- **ONTAP cache volume size**

NetApp recommends enabling volume autosize and scrubbing on cache volumes to maintain optimal size and focus the cache on frequently accessed (hot) data for peak efficiency.

- **ONTAP version compliance**

Upgrade to the latest ONTAP version for full compatibility, support, and access to new features.

Cost optimization

Cost optimization helps you get the most value for your business while keeping costs low.

- **Identify underutilized SSD capacity**

An underutilized SSD capacity tier can incur unnecessary costs. NetApp recommends reducing the SSD tier capacity while maintaining a 20% free space buffer above current used capacity. A decrease operation takes several hours to several days, and other system operations are unsupported during this time.

- **Data tiering policy**

Enable cold data tiering to move cold data from the SSD storage tier to lower-cost storage. Azure Blob Storage serves as the capacity tier for inactive data.

What's next

[Implement well-architected Cloud Volumes ONTAP system configurations](#)

Implement well-architected Cloud Volumes ONTAP system configurations

Using configuration analysis insights and recommendations, leverage NetApp to implement best practices for your Cloud Volumes ONTAP systems running on Microsoft Azure storage. You can easily review the well-architected status, learn about issues with your configurations, and get recommendations to improve the architecture of any systems that aren't optimized for reliability, security, efficiency, performance, and cost.

[Learn about the configuration analysis and well-architected status.](#)

About this task

The well-architected dashboard analyzes Cloud Volumes ONTAP system deployment configurations on Microsoft Azure daily. The daily analysis provides the well-architected status, insights, and recommendations.

Link or Console agent connectivity allows the well-architected dashboard in the NetApp Console to complete a comprehensive scan of your Cloud Volumes ONTAP systems for issues with performance, data protection, and configurations. This ensures that you receive accurate insights and recommendations for optimizing your Cloud Volumes ONTAP systems.

Storage configuration requirements vary. You can dismiss the analysis of specific configurations that don't apply to your storage environment. This helps you avoid unnecessary alerts and inaccurate optimization results.

Before you begin

- You must [add a Cloud Volumes ONTAP system](#) to NetApp Console to view the well-architected status and recommendations for configuration issues.

- You should deploy a [Console agent](#) for the most comprehensive analysis of your system resources.

View recommendations for configuration issues

You can view recommendations for configuration issues after the daily analysis completes. Recommendations explain best practices and potential risks of unoptimized configurations. You can also download a CSV file of the recommendations.

Steps

1. Log in to the [NetApp Console](#).
2. From the NetApp Console menu, select **Workloads** and then **Well-architected**.
3. From the Well-architected dashboard, select **View** for any configuration.

Optionally, select [↓](#) to download a CSV file of the recommendations for all configurations.

4. Review the recommendation.

What's next

Fix configuration issues to keep your systems running at optimal performance.

Build your own rules

Learn about custom rules

Custom rules let you set, check, and enforce your own architecture standards, along with NetApp best practices, in the Well-architected dashboard.

Overview

The Rule builder lets you create custom best-practice rules using plain language. These rules are checked across all of your resources.

Custom rules help you enforce your organization's standards, risk limits, and operational requirements—things that generic vendor rules might not fully cover.

How custom rules work

Custom rules use an AI-guided process that turns your plain-language instructions into clear, structured rules. The AI acts as a translator and checker. It suggests a rule, explains how it understood your request, and asks for your approval before the rule is saved or scheduled.

This process ensures that:

- The rule logic is clearly defined and checked for errors
- No free-form code is run
- You can see exactly what will be evaluated before you approve the rule

Before you begin

Before you can create and run custom rules, ensure you have the following:

AWS credentials

Read-only access to your AWS environment. Custom rules require read-only permissions as a security boundary. [Add AWS credentials to Workload Factory](#).

ONTAP credentials

FSx viewer user with read-only permissions. Workload Factory creates this user automatically with the required permissions.

Link or agent

Required for connectivity to FSx file systems when evaluating rules. [Connect to an FSx for ONTAP file system with a link](#).

Limitations

The following limitations apply to custom rules:

- Automatic fixes are not available. You must correct non-compliant resources yourself using the guidance provided.
- Each rule can check only one type of resource. To check multiple resource types, create separate rules.

- The shortest evaluation interval is 1 hour to avoid excessive scanning.
- Rules have read-only access and cannot make changes to your environment.

Rule definition model

Each custom rule consists of the following components:

Rule name

A user-defined name for the rule.

Description

Your rationale for why this rule matters to your organization.

Resource type

The FSx resource to evaluate (file system, volume, or cache). Currently, one resource type per rule.

Scheduler

How often the rule is evaluated (minimum 1 hour, default 24 hours).

Condition logic

The specific criteria to check.

Evaluation scope

Which resources are evaluated (all applicable resources in scope).

Remediation logic

Manual guidance for addressing non-compliant resources.

Rule lifecycle

Custom rules progress through the following states:

Draft

Rule is being created. No evaluation occurs.

Dry-run

One-time evaluation to preview which resources would be affected. Used for validation before scheduling.

Scheduled (Enabled)

Rule is active and runs on the defined schedule.

Disabled

Rule is paused but not deleted. Can be re-enabled.

Deleted

Rule is permanently removed.

Custom rule examples

The following examples illustrate common custom rules:

Production volume protection

"All volumes with tag 'Prod' must have a snapshot policy installed"

This rule automatically creates snapshots to protect production volumes according to company requirements.

Archive volume tiering

"All volumes with tag 'Archive' should have a tiering policy set to 'All'"

This rule lowers costs by automatically moving archived data to cheaper storage.

File system naming standards

"All file systems must follow the naming convention 'fsx-{environment}-{application}'"

This rule validates that file systems adhere to organizational naming conventions for easier management and cost allocation.

What to do next

[Create a custom rule](#)

Create a custom rule

Create custom rules by describing them in plain language. The AI rule builder turns your request into a validated rule that checks your FSx for ONTAP resources.

Before you begin

- You have configured AWS credentials with read-only access.
- You have ONTAP credentials with viewer permissions.
- You have a link or agent configured for FSx for ONTAP connectivity.
- You understand that custom rule creation uses NetApp's Bedrock AI service.

About this task

The rule creation process walks you through the steps: defining the rule, reviewing how the AI interpreted it, and checking the results before scheduling regular evaluations. You stay in control at every step. The system suggests a rule based on your prompt, but nothing moves forward until you confirm it.

Create a rule

Steps

1. Log in using one of the [console experiences](#).
2. Select the menu  and then select **Well-architected**.
3. From the Well-architected menu, select **Rule builder**.

When you open the rule builder, it shows sample prompts to help you write your custom rule. You can select **Copy prompt** to copy a sample prompt into the AI dialog text box.

4. In the **Create a rule** field, enter your rule description in natural language. Be as specific as possible about:

- What resource type you're checking (file system, volume, or cache).
- What condition you're validating.
- What threshold defines compliance.
- Why this rule matters (optional but recommended).

5. Select .

The AI analyzes your prompt and generates a rule definition.

Review the AI interpretation

The rule builder displays:

- **Parsed interpretation:** How the AI understood your prompt in plain language.
- **Rule definition:** The structured rule including resource type, condition logic, and evaluation criteria.
- **Reasoning:** Why the AI interpreted your prompt this way.
- **Confidence indicator:** How confident the system is in the interpretation.

Steps

1. Review the interpretation to make sure it matches what you intended.

Check that the rule definition is correct.

If the interpretation is unclear or wrong, the system may ask questions such as:

- * Which resource should be checked?
- * What value or limit defines compliance?
- * How often should the rule run?

2. Respond to the AI's clarifying questions.

The AI might ask you to choose from several options to better understand what you need. Answer each question and select **Continue**, or select **Skip** to move past optional questions.

3. After answering all questions, select **Continue** to create your rule.

Test the rule

Before scheduling the rule, run a one-time test to see which resources it will affect.

Steps

1. Select **Validate rule**.

The system evaluates all resources in scope against your rule logic.

2. Review the validation results:

- **Resources evaluated:** Total number of resources checked
- **Compliant:** Resources that meet the rule criteria
- **Non-compliant:** Resources that do not meet the criteria
- **Failed evaluations:** Resources that could not be evaluated (with error details)

3. If some resources failed evaluation, review the error reasons:

- **AWS credential errors:** Read-only permissions may be insufficient for certain resources
- **Connectivity errors:** Link or agent might not be configured for specific file systems
- **ONTAP permission errors:** The viewer user might not have access to certain resources

Save or schedule the rule

After you test your rule, you can save it as a draft or set it to run regularly.

Steps

1. Do one of the following:
 - To schedule regular evaluation, set the evaluation frequency (minimum 1 hour, default 24 hours) and select **Schedule**. The rule is enabled and runs on the defined schedule.
 - To save without scheduling, select **Save as draft**. The rule is saved but not evaluated until you schedule it.
 - To discard the rule, select **Discard** to cancel rule creation and start over.

Result

Your custom rule has been created and is listed in the rule catalog. If you set a schedule, it will check your FSx for ONTAP resources at the specified frequency.

Troubleshooting

No file systems available

Set up your AWS credentials and make sure your environment has at least one FSx for ONTAP file system. The rule builder needs a file system to apply rules.

Low confidence interpretation

More information is needed. Answer the questions or rewrite your prompt with clear details about the resource type, limits, and conditions.

Partial validation failures

Check which resources failed and why. Common causes are missing link or agent settings, or not having enough permissions. Fix the problem, then validate again.

Ambiguous prompt

Be more specific about what you want to check. Include the resource type, the condition, and the threshold. See the prompt examples for help.

Rule targets multiple resource types

Create a separate rule for each resource type. Only one resource type per rule is supported.

What to do next

[Manage custom rules](#)

Manage custom rules

The Rules catalog is one place to manage all your custom rules. You can see each rule's details, check its results, and turn it on or off.

View the Rules catalog

The Rules catalog shows all the rules you created, their status, schedule, and latest results.

Steps

1. Log in using one of the [console experiences](#).
2. Select the menu  and then select **Rule builder**.
3. Click **View your rules** to open the Rules catalog.

View rule results

The results show which resources follow your rule and which do not.

Steps

1. In the Rules catalog, click the rule you want to review.
2. Select the **All runs results** tab.
3. Select **View details** to see the results for each run.

If the check failed for some items, read the error message to see why. Common reasons are connection problems, missing permissions, or a Link/Connector that hasn't been set up.

Pause a rule

Pause a rule to stop evaluations without deleting the rule. Paused rules stay in the catalog and can be restarted at any time.

Steps

1. In the Rules catalog, click the rule you want to pause.
2. Do one of the following:
 - To pause a scheduled rule, click **Pause**, then confirm. The rule stops running on its schedule.
 - To resume a paused rule, click **Resume**, then confirm. The rule resumes regular evaluations.

Delete a custom rule

Delete a rule permanently when you no longer need it. This action cannot be undone.

Steps

1. In the rule catalog, click the rule you want to delete.
2. Click **Delete**.
3. Confirm that you want to permanently delete the rule.

Result

The rule is removed from the catalog. All evaluation history is deleted.

Run a quick test

Run a quick test at any time to check current compliance without waiting for the next scheduled run.

Steps

1. In the Rules catalog, click the rule you want to evaluate.
2. Click **Validate**.

The system evaluates all resources in scope against the rule logic.

3. Review the results to see current compliance status.

Tests are audited and appear in the rule's evaluation history.

Understand execution status

Execution status shows whether a rule ran successfully.

Successful

All relevant resources were checked and no errors were found.

Partially successful

Some resources were checked successfully, but others failed. Check the error details for the ones that could not be checked.

Failed

The evaluation did not finish. Common causes include AWS credential errors, network connection problems, or ONTAP permission issues.

If a rule keeps failing or only partly succeeds, check that:

- AWS credentials have read-only access to all resources.
- Link and connector are configured for all file systems in scope.
- The FSx for ONTAP viewer user has appropriate permissions.

What to do next

[Learn more about custom rules](#)

Legal notices

Legal notices provide access to copyright statements, trademarks, patents, and more.

Copyright

<https://www.netapp.com/company/legal/copyright/>

Trademarks

NETAPP, the NETAPP logo, and the marks listed on the NetApp Trademarks page are trademarks of NetApp, Inc. Other company and product names may be trademarks of their respective owners.

<https://www.netapp.com/company/legal/trademarks/>

Patents

A current list of NetApp owned patents can be found at:

<https://www.netapp.com/pdf.html?item=/media/11887-patentspage.pdf>

Privacy policy

<https://www.netapp.com/company/legal/privacy-policy/>

Open source

Notice files provide information about third-party copyright and licenses used in NetApp software.

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.