



Build your own rules

Well-architected dashboard

NetApp

September 01, 2026

This PDF was generated from <https://docs.netapp.com/us-en/console-well-architected/learn-custom-rules.html> on September 01, 2026. Always check docs.netapp.com for the latest.

Table of Contents

- Build your own rules 1
 - Learn about custom rules in NetApp Console 1
 - Overview 1
 - How custom rules work 1
 - Before you begin 1
 - Limitations 1
 - Rule definition model 2
 - Rule lifecycle 2
 - Custom rule examples 3
 - What to do next 3
 - Create a custom rule in NetApp Console 3
 - Create a rule 3
 - Review the AI interpretation 4
 - Test the rule 4
 - Save or schedule the rule 5
 - Troubleshooting 5
 - What to do next 5
 - Manage custom rules in NetApp Console 6
 - View the Rules catalog 6
 - View rule results 6
 - Pause a rule 6
 - Delete a custom rule 6
 - Run a quick test 7
 - Understand execution status 7
 - What to do next 7

Build your own rules

Learn about custom rules in NetApp Console

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.



If your account administrator has turned off AI features, the Rule builder will not be available and you will not be able to create custom rules. [Learn about managing AI features.](#)

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 in NetApp Console

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.

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.



If your account admin has turned off AI features, you'll see a message and won't be able to create custom rules. Contact your administrator or [learn about AI administration](#).

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.

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 in NetApp Console

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 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 Console agent 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](#)

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.