



Custom rules

Workload Factory for NetApp Console

NetApp
October 07, 2026

Table of Contents

- Custom rules 1
 - Learn about custom rules in NetApp Console 1
 - Overview 1
 - How custom rules work 1
 - Limitations 1
 - Rule definition model 1
 - Rule lifecycle 2
 - Custom rule examples 2
 - What to do next 3
 - Create a custom rule in NetApp Workload Factory 3
 - About this task 3
 - Before you begin 4
 - Create a rule 4
 - Review the AI interpretation 4
 - Test the rule 5
 - Save or schedule the rule 5
 - Troubleshooting 6
 - What to do next 6
 - Manage custom rules for NetApp Workload Factory 6
 - View the Rules catalog 6
 - View rule results 6
 - Edit a custom rule 7

Custom 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

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 Workload Factory

Create custom rules by describing them in plain language. The AI rule builder in NetApp Workload Factory 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 administrator turned off AI features, you won't be able to create custom rules. Contact your administrator or [learn about AI administration](#).

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.

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.

Before you begin

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

- You have configured AWS credentials with read-only access. [Add AWS credentials to Workload Factory](#).
- You have ONTAP credentials with viewer permissions. [Add ONTAP credentials to Workload Factory](#).
- You have a link or Console agent configured connectivity to the cloud storage system. [Create and associate a link](#) or [deploy a Console agent](#).
- You understand that custom rule creation uses NetApp's Bedrock AI service.

Create a rule

Use the Rule builder to create custom best-practice rules using plain language. These rules are checked across all of your resources.

Steps

1. Log in to the [NetApp Console](#).
2. Select the menu , **Workloads > 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 for NetApp Workload Factory

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.

Edit a custom rule

You can change a rule's logic, schedule, or other settings at any time. When you edit a rule, the rule builder opens with the rule's current settings.

Steps

1. In the Rules catalog, click the rule you want to edit.
2. Click **Edit**.

The rule switches to draft mode and the rule builder opens.

3. Edit the rule prompt or use the conversation to improve the rule.
4. Review the AI's updated interpretation and rule definition.

The system shows what changed from the current rule, including any API calls or logic.

5. Do one of the following depending on the changes made:
 - If minor changes were made, click **Save** to update the rule.
 - If significant changes were made, click **Validate rule** to test the changes, then click **Schedule** to save and schedule the rule, or click **Save as draft** to save without scheduling.
 - To discard the changes, click **Revert to previous version**. The rule returns to its original definition and leaves edit mode.