



Administer Workload Factory

Workload Factory for NetApp Console

NetApp

October 07, 2026

Table of Contents

Administer Workload Factory	1
How NetApp Workload Factory supports well-architected workloads	1
Get started with Workload Factory to detect and fix workload misconfigurations	1
Configure NetApp Workload Factory notifications	1
Configure Workload Factory notifications	1
Subscribe to the Amazon SNS topic	3
Filter notifications	3
Notification types and messages	5
Monitor NetApp Workload Factory operations with Tracker	7
Track and monitor operations	7
View API request	7
Retry a failed operation	8
Edit and retry a failed operation	8
Manage NetApp Workload Factory links	8
View the links associated with your account	8
Edit a link	9
Authenticate a link	9
Update the password for link authentication	10
Remove a link	10
Manage AI features for FSx for ONTAP in NetApp Workload Factory	11
About AI features	11
Configuration options	11
Before you begin	12
Configure AI features	12
Budget controls and credit limits	12
AWS GovCloud considerations	13
Impact on existing sessions	13
Related information	13
Custom dashboards for FSx for ONTAP	13
Learn about custom dashboards for FSx for ONTAP in NetApp Workload Factory	13
Create a custom dashboard in NetApp Workload Factory	16
Manage custom dashboards in NetApp Workload Factory	17
Troubleshoot custom dashboards in NetApp Workload Factory	18
Automate tasks using Codebox	19
Learn about Codebox automation in NetApp Workload Factory	19
Use Codebox for automation in NetApp Workload Factory	20
Use CloudShell in NetApp Workload Factory	23
About this task	23
CloudShell commands	24
Before you begin	25
Deploy CloudShell	25
Rename a CloudShell session tab	26
Duplicate CloudShell session tab	27

Close CloudShell session tabs	27
Split CloudShell session tabs	27
Update settings for a CloudShell session	28
Remove credentials from NetApp Workload Factory	28

Administer Workload Factory

How NetApp Workload Factory supports well-architected workloads

Workload Factory helps you maintain and operate reliable, secure, efficient, and cost-effective workload configurations that align with the Well-Architected Framework for your cloud provider. Workload Factory provides daily analysis of your workloads, recommendations, and automatic fixes to promote healthy workload operations. By automating this process, Workload Factory minimizes human error and ensures consistency in workload management.

Unresolved directive in admin/well-architected-workloads.adoc - include::_include/well-architected-workloads.adoc[]

Get started with Workload Factory to detect and fix workload misconfigurations

To get started with Workload Factory, sign up, add credentials, and establish connectivity to manage AWS resources and optimize workloads using Amazon FSx for NetApp ONTAP.

[Quick start](#)

Related information

The following pages provide guidance on implementing well-architected configurations across different NetApp storage solutions:

- [Implement well-architected FSx for ONTAP file systems](#)
- [Implement well-architected database configurations](#)
- [Implement well-architected EVS configurations](#)
- [Implement well-architected NetApp Volumes configurations](#)
- [Implement well-architected Cloud Volumes ONTAP system configurations in Microsoft Azure](#)

Configure NetApp Workload Factory notifications

You can configure the NetApp Workload Factory notification service to send notifications as alerts in NetApp Console, to any email addresses associated with the account, or to an Amazon SNS topic. Notifications sent as alerts appear in NetApp Console when you have a Console agent or link deployed. When Workload Factory publishes notifications to an Amazon SNS topic, subscribers to the topic (such as people or other applications) receive the notifications at the endpoints configured for the topic (such as email or SMS messages).

Configure Workload Factory notifications

You can configure Workload Factory notifications using NetApp Console or the Workload Factory console.

Options for receiving notifications include:

NetApp Console

- **Notifications:** Configure Workload Factory to send notifications that appear under the bell icon in NetApp Console.
- **Email:** Enable email notifications in NetApp Console to receive notifications to any email addresses associated with the account without requiring Amazon SNS configuration.
- **Amazon SNS:** Configure Workload Factory to send notifications to an Amazon SNS topic.

Workload Factory console

- **Email:** Enable email notifications in the Workload Factory console to receive notifications to any email addresses associated with the account without requiring Amazon SNS configuration.
- **Amazon SNS:** Configure Workload Factory to send notifications to an Amazon SNS topic using the Workload Factory console.



When you configure notifications in NetApp Console, it takes ownership of notification delivery and the Workload Factory console notification options are disabled and displayed in read-only mode. A tooltip states that notifications are managed from NetApp Console. You can then manage notifications only from NetApp Console.

Before you begin

The following prerequisites apply only when configuring Amazon SNS notifications:

- You need to configure Amazon SNS and create Amazon SNS topics using either the Amazon SNS console or the AWS CLI.
- Note that Workload Factory supports the **Standard** topic type. This type of topic does not ensure that notifications are sent to subscribers in the order in which they were received, so consider this if you have critical or emergency notifications.

Configure notifications from NetApp Console

Steps

1. Log in to the [NetApp Console](#).
2. From the NetApp Console menu, select **Workloads**, **Administration**, and then **Notifications setup**.
3. On the Notifications setup page, enable one or more of the following notification types:
 - a. **NetApp Console notifications:** Select **Enable NetApp Console notifications** to configure Workload Factory to send notifications in NetApp Console.
 - b. **Email notifications:** Select **Enable email notifications** to configure Workload Factory to send notifications to any email addresses associated with the account.
 - c. **Amazon SNS notifications:** Select **Enable SNS notifications**, then follow the instructions to configure Amazon SNS from the Amazon SNS console.

After you create the topic, copy the topic ARN and enter it in the **SNS topic ARN** field on the **Notifications setup** page.

4. After you verify the configuration by sending a test notification, select **Apply**.

Configure notifications from Workload Factory console

Steps

1. Log in to the [Workload Factory console](#).
2. From the Workload Factory console menu, select **Workloads**, **Administration**, and then **Notifications setup**.
3. Enable one or more of the following notification types:
 - **Email notifications:** Select **Enable email notifications**. Any email addresses associated with the account are displayed in read-only mode.
 - **Amazon SNS notifications:** Select **Enable SNS notifications**, then follow the instructions to configure Amazon SNS from the Amazon SNS console.

After you verify the configuration by sending a test notification, select **Apply**.

Subscribe to the Amazon SNS topic

After you configure Workload Factory to send notifications to a topic, follow the [instructions](#) in the Amazon SNS documentation to subscribe to the topic so that you can receive notifications from Workload Factory.

Filter notifications

You can reduce unnecessary notification traffic and target specific notification types for specific users by applying filters to the notifications. You can do this using an Amazon SNS policy for SNS notifications, and using the notifications settings in NetApp Console.

Filter Amazon SNS notifications

When you subscribe to an Amazon SNS topic, you receive all notifications published to that topic by default. If you want to receive only specific notifications from the topic, you can use a filter policy to control which notifications you receive. Filter policies cause Amazon SNS to deliver only the notifications that match the filter policy to the subscriber.

You can filter Amazon SNS notifications by the following criteria:

Description	Filter policy field name	Possible values
Resource type	resourceType	• DB • Microsoft SQL Server host • PostgreSQL Server host
Workload	workload	WLMDB

Description	Filter policy field name	Possible values
Priority	priority	• Success • Info • Recommendation • Warning • Error • Critical
Notification type	notificationType	• Deployment • Well-architected

Steps

1. In the Amazon SNS console, edit the subscription details for the SNS topic.
2. In the **Subscription filter policy** area, select to filter by **Message attributes**.
3. Enable the **Subscription filter policy** option.
4. Enter a JSON filter policy in the **JSON editor** box.

For example, the following JSON filter policy accepts notifications from the Microsoft SQL Server resource that are related to the WLMDB workload, have a priority of Success or Error, and provide details on Well-architected status:

```
{
  "accountId": [
    "account-a"
  ],
  "resourceType": [
    "Microsoft SQL Server host"
  ],
  "workload": [
    "WLMDB"
  ],
  "priority": [
    "Success",
    "Error"
  ],
  "notificationType": [
    "Well-architected"
  ]
}
```

5. Select **Save changes**.

For other examples of filter policies, refer to [Amazon SNS example filter policies](#).

For further information about creating filter policies, refer to the [Amazon SNS documentation](#).

Filter notifications in NetApp Console

You can use NetApp Console notifications settings to filter notifications that you receive in the Console by severity level, such as Critical, Info, or Warning.

For more information about filtering notifications in the Console, refer to the [NetApp Console documentation](#).

Notification types and messages

Workload Factory sends notifications for the following events:

Event	Description	Notification type	Severity	Workload	Resource type
Some database instances in your account are not well-architected	All Microsoft SQL Server instances in your account have been analyzed for well-architected issues. The description for this event gives the number of well-architected instances and unoptimized instances. Review well-architected status findings and recommendations in the Databases inventory from the Workload Factory console.	Well-architected	Recommendation	Databases	Microsoft SQL Server instance
Microsoft SQL Server/PostgreSQL server deployment succeeded	The deployment of the Microsoft SQL Server or PostgreSQL host succeeded. For more information, go to job monitoring.	Deployment	Success	Databases	FSx for ONTAP, DB host
Microsoft SQL Server/PostgreSQL server deployment failed	The deployment of the Microsoft SQL Server or PostgreSQL host failed. For more information, go to job monitoring.	Deployment	Error	Databases	FSx for ONTAP, DB host
Failed replication relationship creation	A SnapMirror replication relationship creation has failed. For more information, go to Tracker.	Replication	Critical	General storage	FSx for ONTAP
FSx for ONTAP creation failure	An FSx for ONTAP file system creation process has failed. For more information, go to Tracker.	FSx for ONTAP file system action	Critical	General storage	FSx for ONTAP
Automatic SSD capacity or inodes increase success	During a recent automatic capacity management update, the FSx for ONTAP file system either increased SSD capacity or volume inodes successfully. For more information, go to Tracker.	Capacity management	Success	General storage	FSx for ONTAP file

Event	Description	Notification type	Severity	Workload	Resource type
Automatic SSD capacity or inodes increase failure	During a recent automatic capacity management update, the FSx for ONTAP file system failed to increase SSD capacity or volume inodes. For more information, go to Tracker.	Capacity management	Critical	General storage	FSx for ONTAP file systems
FSx for ONTAP issue detected	All FSx for ONTAP file systems have been analyzed for well-architected issues. The scan detected one or more issues. For more information, review the well-architected analysis from the Storage dashboard in the Workload Factory console.	Well-architected analysis	Recommendation	General storage	FSx for ONTAP file systems
Automatic capacity management event for FSx for ONTAP	The SSD performance tier for the FSx for ONTAP file system reached the warning threshold capacity/percentage total.	Capacity management	Warning	General storage	FSx for ONTAP file systems
Automatic inodes management event for FSx for ONTAP	The inode count for the FSx for ONTAP volume reached the warning threshold count/percentage total.	Capacity management	Warning	General storage	FSx for ONTAP file systems
Suspicious volume activity detected in FSx for ONTAP file system	NetApp Autonomous Ransomware Protection with AI (ARP/AI) detected suspicious volume activity.	Ransomware protection	Critical	General storage	FSx for ONTAP file systems
Latency threshold breach detected	One or more volumes in the FSx for ONTAP cluster exceeded the latency threshold.	Performance monitoring	Warning	EDA	FSx for ONTAP file systems
Monthly cost report	Monthly cost summary for your account, showing spending trends, unusual changes, and the best savings opportunities for FSx for ONTAP file systems.	Cost report	Recommendation	General storage	FSx for ONTAP file systems
Replication delay	Replication is taking longer than expected.	Replication	Critical	General storage	FSx for ONTAP file systems
Custom dashboard creation succeeded	Your custom dashboard has been successfully created and is ready to view.	Custom Dashboards	Success	General storage	Workload Factory account
Custom dashboard creation failed	Workload Factory was unable to create your custom dashboard. Try creating the dashboard again.	Custom Dashboards	Error	General storage	Workload Factory account

Monitor NetApp Workload Factory operations with Tracker

Monitor and track the execution of FSx for ONTAP, credentials, and link operations and monitor task progress with Tracker in NetApp Workload Factory.

About this task

Workload Factory provides Tracker, a monitoring feature, so you can monitor and track the progress and status of FSx for ONTAP, credentials, and link operations, review details for operation tasks and subtasks, and diagnose any issues or failures.

Several actions are available in Tracker. You can filter jobs by time frame (last 24 hours, 7 days, 14 days, or 30 days), workload, status, and user; find jobs using the search function; and download the jobs table as a CSV file. You can refresh Tracker at any time. And you can quickly retry a failed operation or edit parameters for a failed operation and try the operation again.

Tracker supports two levels of monitoring depending on the operation. Each task, such as file system deployment, displays the task description, status, start time, task duration, user, region, proxy resource, task ID, and all related sub tasks. You can view API responses to understand what happened during the operation.

Tracker task levels with examples

- Level 1 (task): Tracks file system deployment.
- Level 2 (sub task): Tracks the sub tasks related to the file system deployment.

Operation status

Operation status in Tracker is as follows *in progress*, *success*, and *failed*.

Operation frequency

Operation frequency is based on the job type and the job schedule.

Events retention

Events are retained in the user interface for 30 days.

Track and monitor operations

Track and monitor operations in the NetApp Console with Tracker.

Steps

1. Log in using one of the [console experiences](#).
2. Select the menu  and then select **Administration**.
3. From the Administration menu, select **Tracker**.
4. In Tracker, use the filters or search to narrow job results. You can also download a jobs report.

View API request

View the API request in the Codebox for a task in Tracker.

Steps

1. In Tracker, select a task.
2. Select the actions menu and then select **View API request**.

Retry a failed operation

Retry a failed operation in Tracker. You can also copy the error message of a failed operation.



Only x number of retries are allowed for a failed operation.

Steps

1. In Tracker, select a failed operation.
2. Select the actions menu and then select **Retry**.

Result

The operation is re-initiated.

Edit and retry a failed operation

Edit the parameters of the failed operation and retry the operation outside Tracker.

Steps

1. In Tracker, select a failed operation.
2. Select the actions menu and then select **Edit and retry**.

You are redirected to the operation page where you can edit the parameters and retry the operation.

Result

The operation is re-initiated. Go to Tracker to view the status of the operation.

Manage NetApp Workload Factory links

Manage links that you've associated with your Workload Factory account. You can view links that are associated with an FSx for ONTAP file system or an OCI NetApp Storage Service (OCI NSS) system, provide passwords used for link authentication, and remove links from NetApp Console.

[Learn more about links.](#)

View the links associated with your account

You can view the links that are currently associated with your account.

Steps

1. Select the menu , **Administration > Links**.

Existing links appear on the Links page.

2. To view the storage systems that are associated with a link, select the **View** button in the Associated resources section.
3. If you need the Amazon Resource Name (ARN) for the link, you can select the *copy* icon next to the ARN field.

Edit a link

You can't edit a link from NetApp Console. If you need to make a change to a link, you'll need to create a new link and then associate that link to your storage system.



You can edit the AWS Lambda or Oracle Cloud Functions network configuration (for example VPC, subnets, and security groups) using your cloud provider's console and the changes will be reflected in links or Functions management UI; however, these changes can lead to connectivity issues between AWS Lambda or Oracle Cloud Functions and ONTAP, and are not recommended.

Authenticate a link

Authenticate a link by providing an administrative user password for Workload Factory credentials or with a secret from AWS Secrets Manager or Oracle Vault.

- For AWS Secrets Manager, provide either the secret name or an AWS Secrets Manager secret ARN to connect the link to an FSx for ONTAP file system.



AWS Secrets Manager isn't supported when using a Console agent.

- For Oracle Vault, provide the vault secret OCID to connect the link to an OCI NetApp Storage Service system.



Only one authentication method is supported per link. For example, if you select link authentication with AWS Secrets Manager, you can't change the authentication method later.

Amazon FSx for NetApp ONTAP

Steps

1. Log in to the [NetApp Console](#).
2. Select the menu , **Workloads > Storage > FSx for ONTAP**.
3. From **FSx for ONTAP**, select the actions menu of the file system to associate a link to and then select **Manage**.
4. In the file system overview, select **Authenticate the link**.
5. In the Authenticate link page, select an authenticate mode:
 - **Workload Factory**: enter the password twice.
 - **AWS Secrets Manager**: enter the secret ARN.
6. Select **Apply**.

OCI NetApp Storage Service

Steps

1. Log in to the [NetApp Console](#).
2. Select the menu , **Workloads > Storage > OCI NetApp Storage Service**.
3. From **OCI NetApp Storage Service**, select the actions menu of the storage pool to associate a link to and then select **Manage**.

4. In the storage pool overview, select **Authenticate the link**.
5. In the Authenticate link page, select an authenticate mode:
 - **Workload Factory**: enter the password twice.
 - **OCI Vault**: enter the secret OCID.
6. Select **Apply**.

Result

The link is authenticated, and you can perform advanced ONTAP operations

Update the password for link authentication

When the administrative password is invalid, update the password to connect the link to your storage system.

Amazon FSx for NetApp ONTAP

Steps

1. Log in to the [NetApp Console](#).
2. Select the menu , **Workloads > Storage > FSx for ONTAP**.
3. From **FSx for ONTAP**, select the actions menu of the file system to associate a link to and then select **Manage**.
4. In the file system overview, select **Update password**.
5. In the Authenticate link page, enter the new password twice.
6. Select **Apply**.

OCI NetApp Storage Service

Steps

1. Log in to the [NetApp Console](#).
2. Select the menu , **Workloads > Storage > OCI NetApp Storage Service**.
3. From **OCI NetApp Storage Service**, select the actions menu of the storage pool to associate a link to and then select **Manage**.
4. In the storage pool overview, select **Update password**.
5. In the Authenticate link page, enter the new password twice.
6. Select **Apply**.

Result

The password is updated, and the link is now connected to the storage system.

Remove a link

You can remove a link that you're no longer using in your environment. Any storage systems or other resources that were using the link will be unable to use certain functionality after the link is removed.

Note that the link is only deleted from Workload Factory - it is not deleted from your AWS or Oracle

environment.

- For FSx for ONTAP, you must delete the Lambda function from your AWS account after removing the link in Workload Factory.
- For OCI NetApp Storage Service, you must delete the Function instance from your OCI account after removing the link in Workload Factory.

Amazon FSx for NetApp ONTAP

Steps

1. Log in to the [NetApp Console](#).
2. Select the menu , **Administration > Links**.

Existing links appear on the Links page.

3. From the Links page, select the actions menu of the link to remove and then select **Remove**.
4. If you are sure, select **Remove** again.

Refer to the AWS documentation to [delete the Lambda function](#).

OCI NetApp Storage Service

Steps

1. Log in to the [NetApp Console](#).
2. Select the menu , **Administration > Links**.

Existing links appear on the Links page.

3. From the Links page, select the actions menu of the link to remove and then select **Remove**.
4. If you are sure, select **Remove** again.

Manage AI features for FSx for ONTAP in NetApp Workload Factory

Control access to AI features for FSx for ONTAP in Workload Factory. You can turn off AI features or use AWS Bedrock managed by NetApp.

About AI features

Workload Factory includes several AI-powered features that enhance your experience such as Ask Me, custom dashboards, and analyzers for EMS, database logs, and latency.

As a Workload Factory administrator, you can control how these features use AI on the AI settings page.

Configuration options

Choose from these setup options:

NetApp-managed Bedrock (Recommended)

Use a NetApp-managed AWS Bedrock service. This option is recommended for most users.

- Your data is not used to train models
- Monthly usage credits are shared across your organization
- No additional AWS setup is required

GenAI features off

Turns off all AI features. Users can no longer use Ask Me, analyzers, custom dashboards, rules builder, or other AI-powered tools.

Before you begin

- We recommend that an account admin set up AI features.

Configure AI features

Steps

1. Log in to the [NetApp Console](#).
2. From the NetApp Console menu, select **Workloads > Administration > AI settings**.
3. On the **AI settings** page, select your preferred configuration:
 - **NetApp-managed Bedrock (Recommended)**: Use NetApp-managed AWS Bedrock.
 - **Gen AI features off**: Turn off all AI features.
4. Select **Save preferences**.

Result

Your settings are saved and applied immediately to all AI features in Workload Factory. You can view in Tracker who last updated the settings and when.

If AI features are turned off, users see a message when they try to use AI-powered features. The interface remains visible and clearly shows that the feature is unavailable.

Budget controls and credit limits

NetApp manages budget controls for AI features when using the default, NetApp-managed configuration.

Monthly credit limits

Each account has a monthly spending limit for each AI feature when using NetApp-managed Bedrock.

When budget is reached

If your account reaches the monthly budget limit, Workload Factory will:

- Turn off AI features and gray out related parts of the interface
- Show this message as a tooltip: "Monthly AI credits reached. Contact NetApp Support."
- Log usage for tracking purposes

Request additional credits

If you need more AI credits, contact your NetApp representative. They can adjust your credit limit based on your needs.



To contact your NetApp representative about credit limits, use the in-product chat or visit the [Get help](#) page.

AWS GovCloud considerations

If you create a Workload Factory account in AWS GovCloud (US), note that AI features use AWS Bedrock services in public AWS Regions by default.

If your security requirements do not allow connections to public AWS Region services, you can disable AI features.

Impact on existing sessions

When you change AI settings, any active AI sessions are softly terminated. Current workflows can finish, but new requests use the updated settings.

Termination behavior may vary by feature. See the feature-specific documentation for details.

Related information

- [Learn about Workload Factory features](#)
- [Learn about Custom dashboards](#)
- [Add AWS credentials](#)
- [Permissions reference](#)

Custom dashboards for FSx for ONTAP

Learn about custom dashboards for FSx for ONTAP in NetApp Workload Factory

As a cloud and storage admin, custom dashboards give you a clear view of the systems and workloads you manage. They let you build and personalize views that match your work, priorities, and business goals, instead of being limited to preset layouts.

Custom dashboards use AI to create personalized views of your Workload Factory environment. You simply describe what you want to monitor in plain language, and the system automatically builds visual charts based on your needs.

Everyone in your Workload Factory account can view all custom dashboards. This shared setup helps teams collaborate and see the same operational information across your organization.



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

Why use custom dashboards

Workload Factory users manage many workloads, environments, and priorities, but standard dashboards only show preset views. Custom dashboards help solve several operational challenges:

- **Answer key questions quickly:** Focus on the most important questions or gaps in your understanding instead of general system statistics.
- **Monitor what matters now:** Track the metrics that match your current priorities, not a fixed set of health indicators.
- **Link technical data to business results:** Show how system performance affects operations and business goals.
- **Avoid switching between tools:** View all relevant information in one place—no need to switch between tools, pages, or exports.

What you can do with custom dashboards

During setup, the AI-guided dialog helps you define:

- Workloads and resources to monitor
- Key metrics that matter for your work
- Time ranges and periods to compare
- Views by region, workload, or other categories
- Rules or requirements you need to track and show

View and share dashboards

New dashboards are private by default, so only you can see them. You can make a dashboard public at any time to share it with your team.

- **Private dashboards:** Only you can view these dashboards. Use them for personal monitoring, testing, or work in progress.
- **Public dashboards:** Everyone in your Workload Factory account can view these dashboards. Use them to share monitoring views and keep your team aligned on workloads, priorities, and business goals.

Each dashboard card shows whether the dashboard is private or public, so you can quickly see which dashboards are shared.

[Learn how to change dashboard visibility.](#)

Considerations and limitations

AWS credentials and permissions

To create or view custom dashboards, you need the correct AWS IAM permissions for the resources you want to monitor. Make sure the Workload Factory account has read access to the data sources used by the dashboards.

To build dashboards, Workload Factory uses read-only AWS credentials. These credentials allow only read actions, such as `fsx:DescribeVolumes` and `fsx:DescribeFileSystems`, for the following services: EC2, FSx, CloudWatch, Resource Groups Tagging API, Backup, CloudWatch Logs, KMS, and EFS.

[Learn how to add AWS credentials and set up IAM permissions.](#)

Link to FSx for ONTAP

Workload Factory requires a link to connect to FSx for ONTAP file systems. A link creates a trust relationship and connectivity between Workload Factory and one or more FSx for ONTAP file systems. This enables you to monitor and manage certain file system features directly from the ONTAP REST API calls that are not available through the Amazon FSx for ONTAP API.

[Learn how to create a link.](#)

Read-only design

Custom dashboards are read-only. They cannot change your storage or workload settings. This lets you monitor your system without accidentally changing anything.

Limitations

The following limitations currently apply to custom dashboards:

- You cannot share dashboards outside your Workload Factory account. All dashboard sharing is limited to users within the same Workload Factory account.

Demo environment

If you're using a Workload Factory demo account, some prebuilt dashboards are available. They help you see what custom dashboards can do. Each dashboard shows a common monitoring need: disaster recovery status, capacity and costs across regions, and whether storage protection rules are being followed.

Sample prompts

The following examples show how to describe your monitoring needs in plain language:

- **Disaster recovery monitoring:** "I am setting up a disaster recovery solution in AWS for my on-premises systems. I want to see a complete list of my on-prem resources and the status of each one at the disaster recovery site in the US East region, including whether it is configured, active, and healthy."
- **Multi-region capacity and cost:** "I manage storage across several cloud regions and applications. I want clear visibility into how much storage I have allocated, how much is being used, and what it costs, with details for each region and each application."
- **Storage protection compliance:** "I am setting up a new storage protection strategy based on my organization's standards. Show me all file systems and whether they meet these requirements:
 - Database workloads: 12 daily snapshots per volume and 2 tamper-proof snapshots per week.
 - NFS and SMB shares: 7 daily snapshots per volume and 1 tamper-proof snapshot per week.
 - ARP must be enabled on all volumes."

Next steps

- [Create a custom dashboard](#)
- [Manage custom dashboards](#)
- [Troubleshoot custom dashboards](#)

Create a custom dashboard in NetApp Workload Factory

Create custom dashboards by describing what you want to monitor in plain language. The AI guides you through the setup so your dashboards match your workloads and priorities.

About this task

Custom dashboards use an AI-guided dialog to understand what you want to visualize. You describe your monitoring needs in natural language, and the system asks clarifying questions to ensure the dashboard meets your requirements.

Once created, you can refresh the dashboard to see updated data.

Remember that custom dashboards are read-only by design and cannot make changes to your storage or workload configurations.



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

Create a dashboard

Steps

1. Log in to the [NetApp Console](#).
2. From the NetApp Console menu, select **Workloads > Workloads Overview > Custom dashboards**.

If this is your first dashboard, you'll see a blank screen with sample prompts to help you get started. You can select **Copy prompt** to copy a sample prompt into the AI dialog text box.

3. Select **Create new dashboard**.
4. In the AI dialog, describe what you want to monitor.

Describe it in plain language. The AI will ask a few questions to better understand your needs.

5. Select .
6. 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.

7. After answering all questions, select **Continue** to create your dashboard.

Your dashboard is being created. This might take a moment.

Result

Your custom dashboard is created and added to the dashboard catalog. By default, the dashboard is private and only visible to you. You can change the visibility to public if you want to share it with other users in your Workload Factory account. [Learn how to change dashboard visibility](#).

You'll get a notification when your dashboard is ready. If it can't be created, you'll get a notification with a link to try again. [Learn about configuring notifications](#).

What's next

After creation, you can:

- Change dashboard visibility to share with your team
- Refresh dashboard data to see the latest information
- Delete dashboards you no longer need
- View dashboard details, including who created it and when it was last updated

Related information

- [Manage your custom dashboards](#)
- [Troubleshoot custom dashboards](#)

Manage custom dashboards in NetApp Workload Factory

Manage your custom dashboards from the dashboard catalog. From there, you can view details, share dashboards, refresh data, or delete dashboards you no longer need.

About this task

You can view and manage custom dashboards from the dashboard catalog. Private dashboards are only visible to you, while public dashboards are visible to all users in your Workload Factory account. Each dashboard shows basic details such as the creator's name, the creation date, and a visibility label (Private or Public).

Custom dashboards are read-only. They cannot change your storage or workload settings.

Before you begin

You must have at least one custom dashboard in your Workload Factory account.

Access the dashboard catalog

Steps

1. Log in to the [NetApp Console](#).
2. From the NetApp Console menu, select **Workloads > Workloads Overview > Custom dashboards**.

The dashboard catalog shows all custom dashboards in your Workload Factory account.

3. Review the dashboard list.

Change dashboard visibility

Make a dashboard public to share it with your team. Make it private to stop sharing it.

Steps

1. In the **Custom dashboards** page, locate the dashboard you want to update.
2. From the **Actions** drop-down menu  for that dashboard, select one of the following:
 - **Share dashboard** - Makes the dashboard visible to all users in your Workload Factory account
 - **Change to private dashboard** - Makes the dashboard visible only to you

Result

The dashboard updates immediately. The visibility label on the dashboard card shows the current status.

Refresh dashboard data

Dashboard data loads when you open a dashboard. You can refresh it to see the latest information.

The dashboard reloads data from your workloads. The last updated time changes to show when the data was refreshed.

Delete a dashboard

Delete dashboards you no longer need. This action is permanent and cannot be undone.

Steps

1. In the **Custom dashboards** page, locate the dashboard you want to remove.
2. From the **Actions** drop-down menu for that dashboard, select **Delete**.
3. Confirm the deletion.

Result

The dashboard is permanently removed from your Workload Factory account, and all users lose access to it.

Related information

- [Create additional custom dashboards](#)
- [Troubleshoot custom dashboards](#)

Troubleshoot custom dashboards in NetApp Workload Factory

Use this information to resolve common issues you might encounter when creating or using custom dashboards.

Dashboard creation failed

Problem: You see the error message “Failed to understand request and generate code” when creating a dashboard.

Cause: The system could not understand your request or could not create the visualization from your prompt.

Solution: Try the following:

- Rewrite your request with clearer details about what you want to monitor.
- Start with one of the sample prompts in [Create a custom dashboard](#).
- Break complex monitoring needs into several simpler dashboards.
- Specify the workloads, metrics, time ranges, or dimensions you want to track.

Dashboard failed to load data

Problem: The dashboard was created, but it shows errors when loading data.

Cause: This usually happens because of permission problems or unavailable data sources.

Solution:

- **Check permissions:** Make sure your Workload Factory account has read access to the workloads and resources used by the dashboard. Review the permissions requirements in [AWS credentials and permissions](#).
- **Verify credentials:** Confirm that your AWS credentials are valid and have not expired. See [Add AWS credentials](#) for details.

Dashboard not loading or loading slowly

Problem: The dashboard loads slowly or some widgets do not appear.

Cause: Slow loading can be caused by network issues, large amounts of data, or temporary service delays.

Solution:

- **Check your internet connection:** Make sure your internet connection is stable.
- **Refresh your browser:** Try refreshing the page to see if the dashboard loads correctly.
- **Clear your browser cache and cookies:** This can help resolve loading issues caused by outdated or corrupted data.
- **Wait and try again:** If the problem continues, wait a few minutes and try again.

Missing dashboards

Problem: A dashboard you created is no longer listed in the dashboard catalog.

Cause: Another user in your Workload Factory account might have deleted it.

Solution:

- Make sure you are logged into the correct Workload Factory account.
- Ask other users in your account if someone deleted the dashboard.
- If necessary, recreate the dashboard using the original requirements.

All users in a Workload Factory account can view and delete custom dashboards. Coordinate with your team when managing shared dashboards.

Additional help

If you continue to experience issues with custom dashboards, see [Get help](#) for information about contacting NetApp support.

Automate tasks using Codebox

Learn about Codebox automation in NetApp Workload Factory

Codebox is an Infrastructure as Code (IaC) co-pilot that helps developers and DevOps generate the code needed to execute any operation supported by NetApp Workload Factory. Codebox is aligned with the Workload Factory permission policies and it sets a clear path for execution readiness as well as providing an automation catalog for quick

future reuse.

Codebox capabilities

Codebox provides two key IaC capabilities:

- *Codebox Viewer* shows the IaC that is generated by a specific job flow operation by matching entries and selections from the graphical wizard or from the conversational chat interface. While Codebox Viewer supports color coding for easy navigation and analysis, it does not allow editing—only copying or saving code to the Automation Catalog.
- *Codebox Automation Catalog* shows all saved IaC jobs, allowing you to easily reference them for future use. Automation catalog jobs are saved as templates and shown in context of the resources that apply to them.

Additionally, when setting up Workload Factory credentials, Codebox dynamically displays the AWS permissions that are needed to create IAM policies. The permissions are provided for each Workload Factory capability that you plan to use (databases, AI, FSx for ONTAP, and so on), and they are customizable. You just copy the permissions from Codebox and then paste them in the AWS Management Console so that Workload Factory has the correct permissions to manage your workloads.

Supported code formats

The supported code formats include:

- Workload Factory REST APIs
- AWS CLI
- AWS CloudFormation
- Terraform

Related information

[Learn how to use Codebox.](#)

[Workload Factory REST API documentation.](#)

Use Codebox for automation in NetApp Workload Factory

You can use Codebox to generate the code needed to execute any operation supported by NetApp Workload Factory. You can generate code that can be consumed and run using Workload Factory REST APIs, the AWS CLI, and AWS CloudFormation.

Codebox is aligned with the Workload Factory permission policies by populating the appropriate data in the code based on the AWS permissions provided in the Workload Factory account for each user. The code can be used like a template where you can fill in missing information (for example, credentials) or customize certain data before running the code.

How to use Codebox

As you enter values in user interface wizards in the NetApp Console, you can see the data update in Codebox as you complete each field. When you complete the wizard, but before you select the **Create** button at the bottom of the page, select  to copy in Codebox to capture the code required to build your configuration. For example, this screenshot from creating a new Microsoft SQL Server shows the wizard entries for VPC and

availability zones and the equivalent entries in Codebox for a REST API implementation.

The screenshot shows the 'Create new Microsoft SQL server' console. On the left, the 'Region & VPC' section is set to 'us-east-1 | US East (N. Virginia)' and 'VPC-1 | 172.30.0.0/20'. The 'Availability zones' section shows two nodes: Node 1 with 'us-east-1d' and 'HCL-CC-1 | 192.168.16.0/24', and Node 2 with 'us-east-2d' and 'HCL-CC-2 | 192.168.17.0/24'. On the right, the 'Codebox' panel shows a REST API configuration with a 'Copy' button. The REST API configuration includes a curl command and a JSON body for the network configuration.

With some code formats you can also select the download button to save the code in a file that you can bring to another system. If required, you can edit the code after it has been downloaded so that you can adapt it to other AWS accounts.

Use CloudFormation code from Codebox

You can copy the CloudFormation code generated from Codebox and then launch the Amazon Web Services CloudFormation stack in your AWS account. CloudFormation will perform the actions that you defined in the Workload Factory UI.

The steps to use the CloudFormation code might be different depending on whether you are deploying an FSx for ONTAP file system, creating account credentials, or performing other Workload Factory actions.

Note that the code within a CloudFormation-generated YAML file expires after 7 days for security reasons.

Before you begin

- You'll need to have credentials to log in to your AWS account.
- You'll need to have the following user permissions to use a CloudFormation stack:

▼ Details

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "cloudformation:CreateStack",
        "cloudformation:UpdateStack",
        "cloudformation>DeleteStack",
        "cloudformation:DescribeStacks",
        "cloudformation:DescribeStackEvents",
```

```

        "cloudformation:DescribeChangeSet",
        "cloudformation:ExecuteChangeSet",
        "cloudformation:ListStacks",
        "cloudformation:ListStackResources",
        "cloudformation:GetTemplate",
        "cloudformation:ValidateTemplate",
        "lambda:InvokeFunction",
        "iam:PassRole",
        "iam:CreateRole",
        "iam:UpdateAssumeRolePolicy",
        "iam:AttachRolePolicy",
        "iam:CreateServiceLinkedRole"
    ],
    "Resource": "*"
}
]
}

```

Steps

1. After you have used NetApp Console to define the operation that you want to perform, copy the code in the Codebox.
2. Select **Redirect to CloudFormation** and the Redirect to CloudFormation page is displayed.
3. Open another browser window and log in to the AWS Management Console.
4. Select **Continue** from the Redirect to CloudFormation page.
5. Log in to the AWS account where the code should be run.
6. On the Quick create stack page, under Capabilities, select **I acknowledge that AWS CloudFormation might**
7. Select **Create stack**.
8. Monitor the progress from AWS or from Workload Factory.

Use REST API code from Codebox

You can use the Workload Factory REST APIs generated from Codebox to deploy and manage your FSx for ONTAP file systems and other AWS resources.

You can run the APIs from any host that supports curl and that has internet connectivity.

Note that the authentication tokens are hidden in Codebox, but they are populated when you copy and paste the API call.

Steps

1. After you have used NetApp Console to define the operation that you want to perform, copy the API code in the Codebox.
2. Paste the code and run it on your host system.

Use AWS CLI code from Codebox

You can use the Amazon Web Services CLI generated from Codebox to deploy and manage your FSx for ONTAP file systems and other AWS resources.

Steps

1. After you have used NetApp Console to define the operation that you want to perform, copy the AWS CLI in the Codebox.
2. Open another browser window and log in to the AWS Management Console.
3. Paste the code and run it.

Use Terraform from Codebox

You can use Terraform to deploy and manage your FSx for ONTAP file systems and other AWS resources.

Before you begin

- You'll need a system where Terraform is installed (Windows/Mac/Linux).
- You'll need to have credentials to log in to your AWS account.

Steps

1. After you have used NetApp Console to define the operation that you want to perform, download the Terraform code from the Codebox.
2. Copy the downloaded script archive to the system where Terraform is installed.
3. Extract the zip file and follow the steps in the README.md file.

Use CloudShell in NetApp Workload Factory

Open CloudShell to execute AWS or ONTAP CLI commands from anywhere in the NetApp Workload Factory console.

About this task

CloudShell allows you to execute AWS CLI commands or ONTAP CLI commands in a shell-like environment from within the Workload Factory console. It simulates terminal sessions in the browser, providing terminal features and proxying messages through Workload Factory's backend. It allows you to use the AWS credentials and ONTAP credentials that you have provided in your NetApp account.

CloudShell features include:

- Multiple CloudShell sessions: deploy multiple CloudShell sessions at one time to issue several sequences of commands in parallel,
- Multiple views: split CloudShell tab sessions so you can view two or more tabs horizontally or vertically at the same time
- Session renaming: rename sessions as needed
- Last session content persistence: re-open the last session if you close it by mistake
- Settings preferences: change the font size and output type
- AI-generated error responses for ONTAP CLI commands

- Autocomplete support: start typing a command and use the **Tab** key to view available options



If your account administrator has turned off AI features, AI-generated error responses will not be available. [Learn about managing AI features.](#)

CloudShell commands

Within the CloudShell GUI interface, you can enter `help` to view available CloudShell commands. After you issue the `help` command, the following reference appears.

Description

NetApp CloudShell is a GUI interface built into NetApp Workload Factory enables you to execute AWS CLI commands or ONTAP CLI commands in a shell-like environment. It simulates terminal sessions in the browser, providing terminal features and proxying messages through the backend in Workload Factory. It enables you to use the AWS credentials and ONTAP credentials that you have provided in your NetApp account.

Available commands

- `clear`
- `help`
- `[--fsx <fsxId>] <ontap-command> [parameters]`
- `aws <aws-command> <aws-sub-command> [parameters]`

Context

Each terminal session runs in a specific context: credentials, region, and optionally FSx for ONTAP file system.

+

All AWS commands execute in the provided context. AWS commands will only succeed if the provided credentials have permissions in the specified region.

+

You can specify ONTAP commands with an optional `fsxId`. If you provide an `fsxId` with an individual ONTAP command, then this ID overrides the ID in the context. If the terminal session doesn't have an FSx for ONTAP file system ID context, then you must provide `fsxId` with each ONTAP command.

+

To update different context specifics, do the following:

- * To change credentials: `"using credentials <credentialId>"`
- * To change region: `"using region <regionCode>"`
- * To change FSx for ONTAP file system: `"using fsx <fileSystemId>"`

Showing Items

- To show available credentials: `"show credentials"`
- To show available regions: `"show regions"`
- To show command history: `"show history"`

Variables

The following are examples of setting and using variables. If a variable value contains spaces, you should set it inside quotes.

+

- * To set a variable: `$<variable> = <value>`
- * To use a variable: `$<variable>`
- * Example setting a variable: `$svm1 = svm123`
- * Example using a variable: `--fsx FileSystem-1 volumes show --vserver $svm1`
- * Example setting a variable with string value `$comment1 = "A comment with spaces"`

Operators

Shell operators such as pipe `|`, background execution `&`, and redirection `>` aren't supported. Command execution fails if you include these operators.

Before you begin

CloudShell works in the context of your AWS credentials. To use CloudShell, you must provide at least one AWS credential.



CloudShell is available for you to execute any AWS or ONTAP CLI command. However, if you want to work within the context of an FSx for ONTAP file system, make sure you issue the following command: `using fsx <file-system-name>`.

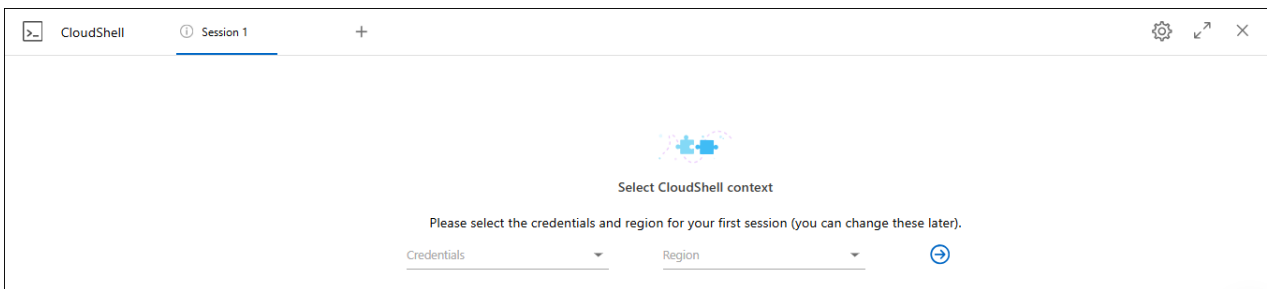
Deploy CloudShell

You can deploy CloudShell from anywhere in the NetApp Workload Factory console. You can also deploy CloudShell from the NetApp Console.

Deploy from Workload Factory console

Steps

1. Log in to the [NetApp Console](#).
2. From the NetApp Console menu, select **Workloads > Administration > CloudShell**.
3. In the CloudShell window, select credentials and region for the CloudShell session and then select the arrow to continue.



4. Enter `help` to view available [CloudShell commands](#) and instructions or refer to the following CLI reference documents for available commands:
 - [AWS CLI reference](#): For commands related to FSx for ONTAP, select **fsx**.
 - [ONTAP CLI reference](#)
5. Issue commands within the CloudShell session.

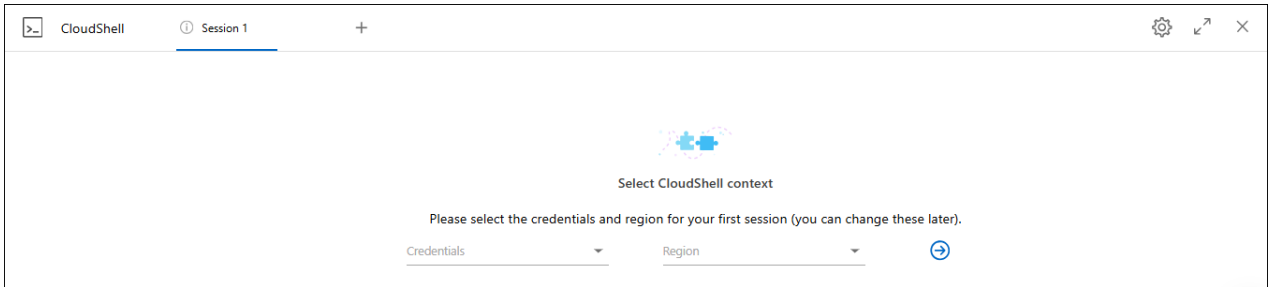
If an error occurs after issuing an ONTAP CLI command, select the light bulb icon to get a brief AI-generated error response with a description of the failure, the cause of the failure, and a detailed

resolution. Select **Read more** for more details.

Deploy from the NetApp Console

Steps

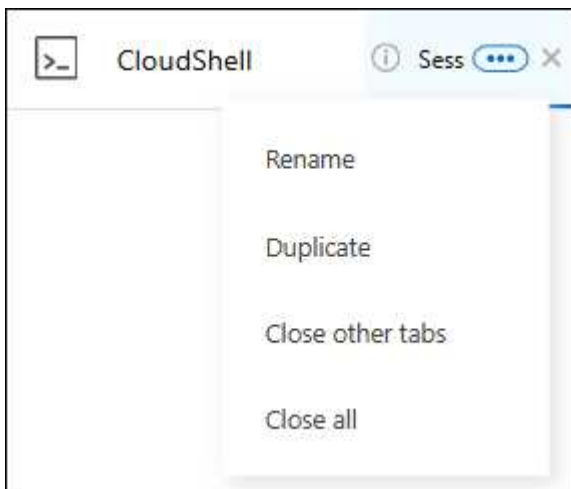
1. Log in to the [NetApp Console](#).
2. From the NetApp Console menu, select **Workloads > Administration > CloudShell**.
3. In the CloudShell window, select credentials and region for the CloudShell session and then select the arrow to continue.



4. Enter `help` to view available CloudShell commands and instructions or refer to the following CLI reference documents for available commands:
 - [AWS CLI reference](#): For commands related to FSx for ONTAP, select **fsx**.
 - [ONTAP CLI reference](#)
5. Issue commands within the CloudShell session.

If an error occurs after issuing an ONTAP CLI command, select the light bulb icon to get a brief AI-generated error response with a description of the failure, the cause of the failure, and a detailed resolution. Select **Read more** for more details.

The CloudShell tasks shown in this screenshot can be completed by selecting the actions menu of an open CloudShell session tab. The instructions for each of these tasks follows.



Rename a CloudShell session tab

You can rename a CloudShell session tab to help you identify the session.

Steps

1. Select the actions menu of the CloudShell session tab.
2. Select **Rename**.
3. Enter a new name for the session tab and then click outside the tab name to set the new name.

Result

The new name appears in the CloudShell session tab.

Duplicate CloudShell session tab

You can duplicate a CloudShell session tab to create a new session with the same name, credentials, and region. The code from the original tab isn't duplicated in the duplicated tab.

Steps

1. Select the actions menu of the CloudShell session tab.
2. Select **Duplicate**.

Result

The new tab appears with the same name as the original tab.

Close CloudShell session tabs

You can close CloudShell tabs one at a time, close other tabs you're not working on, or close all tabs at once.

Steps

1. Select the actions menu of the CloudShell session tab.
2. Select one of the following:
 - Select "X" in the CloudShell tab window to close one tab at a time.
 - Select **Close other tabs** to close all other tabs that are open except the one you're working on.
 - Select **Close all tabs** to close all tabs.

Result

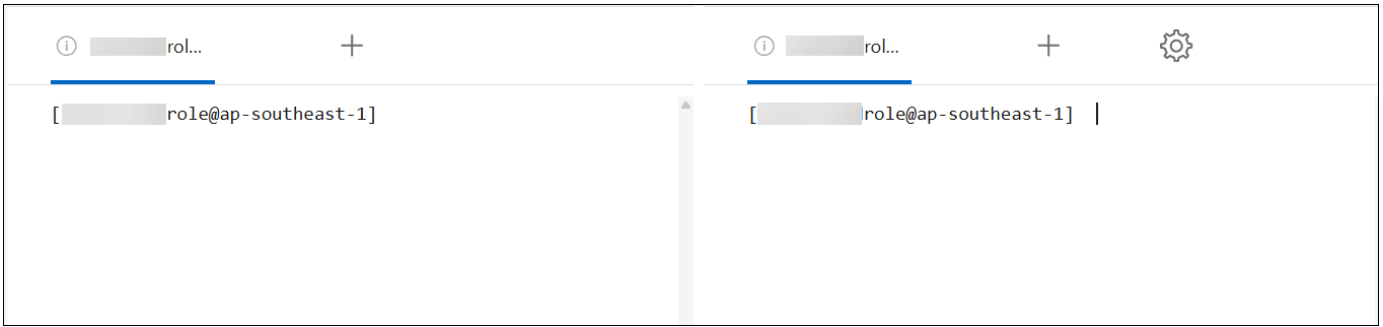
The selected CloudShell session tabs close.

Split CloudShell session tabs

You can split CloudShell session tabs to view two or more tabs at the same time.

Step

Drag and drop CloudShell session tabs to the top, bottom, left, or right of the CloudShell window to split the view.



Update settings for a CloudShell session

You can update font and output type settings for CloudShell sessions.

Steps

1. Deploy a CloudShell session.
2. In the CloudShell tab, select the settings icon.

The settings dialog appears.

3. Update font size and output type as needed.



Enriched output applies to JSON objects and table formatting. All other output appears as plain text.

4. Select **Apply**.

Result

The CloudShell settings are updated.

Remove credentials from NetApp Workload Factory

If you no longer need a set of credentials, you can delete them from Workload Factory. You can only delete credentials that aren't associated with an FSx for ONTAP file system.

Steps

1. Log in to the [NetApp Console](#).
2. From the NetApp Console menu, select **Workloads > Administration > Credentials**.
3. On the **Credentials** page, do the following:
 - In the Workload Factory console, select the action menu for a set of credentials and then select **Remove**. Select **Remove** to confirm.
 - In the NetApp Console, select the action menu for a set of credentials and then select **Delete**. Select **Delete** to confirm.

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.