



Google Cloud NetApp Volumes

Workload Factory for NetApp Console

NetApp
October 07, 2026

This PDF was generated from <https://docs.netapp.com/us-en/data-services-workloads/gcnv/learn-netapp-volumes.html> on October 07, 2026. Always check docs.netapp.com for the latest.

Table of Contents

- Google Cloud NetApp Volumes 1
 - Learn about Google Cloud NetApp Volumes 1
 - Features 1
 - Cost 1
 - Supported regions 1
 - Getting help 1
 - Related links 1
 - Quick start for Google Cloud NetApp Volumes 1
 - Set up Google Cloud NetApp Volumes 2
 - Set up a service account 3
 - Shared VPC 3
 - Troubleshooting 4
 - Assign Google Cloud NetApp Volumes roles 4
 - Assign roles to the service account member 4
 - Add Google Cloud NetApp Volumes credentials to NetApp Workload Factory 5
 - Overview 5
 - Configuration analysis for Google Cloud NetApp Volumes 6
 - Analysis requirements 7
 - Best practices and recommendations for storage workloads 7
 - Implement well-architected Google Cloud NetApp Volumes configurations 8
 - About this task 8
 - Before you begin 8
 - View recommendations for configuration issues 8
 - Dismiss a configuration analysis 8
 - Reactivate a dismissed configuration analysis 9

Google Cloud NetApp Volumes

Learn about Google Cloud NetApp Volumes

Google Cloud NetApp Volumes is a fully managed, cloud-based data storage service that provides advanced data management capabilities and highly scalable performance.

NetApp Volumes helps to accelerate deployment times, manage your workloads and applications, and migrate workloads to the cloud while keeping the performance and features of on-premises storage.

Features

- Runs enterprise apps faster and more efficiently.
- Reduces cloud storage costs by up to 90%.
- Meets mandates for uptime, availability, and security.
- Supports NFS, SMB and multiprotocol environments.

Cost

Volumes created by Google Cloud NetApp Volumes are charged to your subscription to the service, not through the NetApp Console.

There are no charges to discover a Google Cloud NetApp Volumes region or volume from the NetApp Console.

Supported regions

[View supported Google Cloud NetApp Volumes regions](#)

Getting help

For technical support, log a request via the Google Cloud portal. Choose your Google Cloud subscription and the **Google Cloud NetApp Volumes** service under **Storage**. Complete the required information.

For general questions about Google Cloud NetApp Volumes, email NetApp's Google Cloud Team at gcinfo@netapp.com.

For technical issues associated with your cloud volumes, you can create a technical support case from the Google Cloud Console. See [obtaining support](#) for details.

Related links

- [Google Cloud NetApp Volumes documentation](#)
- [NetApp Console Copy and Sync documentation](#)

Quick start for Google Cloud NetApp Volumes

Get started with Google Cloud NetApp Volumes by setting up Google Cloud, and then creating a system.

1

Set up Google Cloud NetApp Volumes

From Google, create a service account.

2

Assign roles

To start working with Google Cloud NetApp Volumes, you must have the appropriate permissions and the Google Cloud NetApp Volumes admin or Google Cloud NetApp viewer role assigned to you.

Add new roles

Associate role in organization, folder, or project

Add role

Organization, folder or project	Category	Role
test-workspace	Application	Google Cloud NetApp Volumes admin

Add new roles

Cancel

From the NetApp Console, assign the correct roles to members.

3

Add a system

From the NetApp Console, click **Add System** and then **Google Cloud Platform** and then **Google Cloud NetApp Volumes** and then **Discover**. Provide the details about the service account and Google Cloud project.

Set up Google Cloud NetApp Volumes

The NetApp Console needs the right permissions through a Google Cloud service account.

Complete the following tasks so that NetApp Console can access your Google Cloud project.



You can use the Google Cloud console or the gcloud CLI for these tasks. To use the gcloud CLI, you must have [installed the Google Cloud CLI](#) first.

- If you do not already have an existing service account, create a new one.
- Grant access for impersonation.
- Grant the IAM role in the shared project.

Set up a service account



Google Cloud project permissions changes might take a couple of minutes to take effect.

1. In the Google Cloud console, [go to the Service accounts page](#).
2. Click **Select a project**, choose your project, and click **Open**.
3. To create a service account, do the following:
 - a. Click **Create service account**.
 - b. Enter the service account name (friendly display name) and description.

The Google Cloud Console generates a service account ID based on this name. Edit the ID if necessary - you cannot change the ID later.
 - c. Click **Create and continue**.
 - d. From the Role list, select the **Google Cloud NetApp Volumes Admin** or **Google Cloud NetApp Volumes Viewer** role.
 - e. Select **Continue**.

Alternatively, you can assign the role using the gcloud CLI:

```
gcloud projects add-iam-policy-binding <YOUR_PROJECT_ID>
--member="serviceAccount:<YOUR_SA_EMAIL>" --role="roles/netapp.admin"
```

- f. Grant impersonation access to this service account: [credentials-sa@wf-production-netapp.iam.gserviceaccount.com](#). For details, see [Create a self-signed JSON Web Token \(JWT\)](#).

The service account owned by NetApp is used to request a short-lived access token that lets you act as that service account without needing access to its private key.

Alternatively, you can grant impersonation access using the gcloud CLI:

```
gcloud iam service-accounts add-iam-policy-binding <YOUR_SA_EMAIL>
--member="serviceAccount:credentials-sa@wf-production
-netapp.iam.gserviceaccount.com"
--role="roles/iam.serviceAccountTokenCreator"
--project=<YOUR_PROJECT_ID>
```

- g. Click **DONE** at the bottom of the page, and continue to the next step.

Shared VPC

In each additional Google Cloud project that will use the service account, do the following:

1. In the *IAM page*, select the Shared VPC host project from the project dropdown menu.
2. Click **Add Principal**.
3. In the New principals field, enter the email address of your service account.

4. From the Select a role dropdown, choose the **Google Cloud NetApp Volumes admin** role.
5. Click **Save**.

Alternatively, you can add the IAM policy binding using the gcloud CLI:

```
gcloud projects add-iam-policy-binding <SHARED_VPC_HOST_PROJECT_ID>
--member="serviceAccount:<YOUR_SA_EMAIL>" --role="roles/netapp.admin"
```

For detailed steps, refer to Google Cloud documentation:

- [Creating and managing service accounts](#)
- [Google Cloud NetApp Volumes roles and permissions](#)
- [Granting, changing, and revoking access to resources](#)

Troubleshooting

If you encounter an error, the **iam.disableCrossProjectServiceAccountUsage** policy might be enforced. To fix this, do the following:

1. In the Google Cloud console, go to the [Organization policies page](#).
2. Find the **Disable cross-project service account usage** policy and disable it.

What's next?

[Assign Google Cloud NetApp Volumes roles.](#)

Assign Google Cloud NetApp Volumes roles

You must assign the correct roles to members in NetApp Console to start working with Google Cloud NetApp Volumes. For details, see [Learn about NetApp Console access roles for all services](#).

Assign roles to the service account member

1. Log into the [NetApp Console](#).
2. Select **Administration** and then **Identity and access**.
3. Select the actions menu  next to the member that you want to assign a role and select **Add a role**.
4. To add a role, complete the steps in the dialog box:

- a. Select folder or project: Choose the level of your resource hierarchy that the member should have permissions for.

If you select a folder, the member has permissions to everything that resides within the folder.

- b. From the **Category** drop down, select the **Application** role category.
[Learn about access roles.](#)
- c. From the **Role** drop down, select a role that provides the member with permissions for the resources that are associated with the folder or project that you selected.

Important: You must add one or both of these roles:

- *Google Cloud NetApp Volumes admin*
OR
- *Google Cloud NetApp Volumes viewer*

d. Add role: If you want to provide access to additional folders or projects within your organization, select **Add role**, specify another folder or project or role category, and then select a role category and a corresponding role.

5. Select **Add new roles**.

What's next?

[Add a Google Cloud NetApp Volumes system.](#)

Add Google Cloud NetApp Volumes credentials to NetApp Workload Factory

Add and manage your cloud provider credentials so that NetApp Workload Factory has the permissions that it needs to deploy and manage resources in your cloud provider accounts.

Overview

You can add Google Cloud NetApp Volumes credentials from the Credentials page in NetApp console. The console provides guided setup instructions and a documentation link so you can complete the required Google Cloud configuration and then return to finish adding the credentials.

Use this workflow to grant Workload Factory the permissions that it needs to discover, analyze, and manage resources in your Google Cloud environment.

There are three parts to creating the credentials:

- Step 1: Select the permissions level that you want to grant to Workload Factory.
- Step 2: Create and validate a Google Cloud service account, and then select the Google Cloud project to manage.
- Step 3: Enter a credentials name and add the credentials.

Before you begin

You'll need to have credentials to log in to your Google Cloud account.

Steps

1. Log in to the [NetApp console](#).
2. From the menu, select **Workloads > Administration > Credentials**.
3. On the Credentials page, select **Add credentials**.
4. Select **Google Cloud NetApp Volumes** as the cloud provider.
5. On the Add Google Cloud NetApp Volumes credentials page, complete each section under **Permissions configuration**.

Step 1: Create permission policies

Steps

1. Under **Create permission policies**, **View, plan, and analyze** is selected by default. This permission policy allows you to view Google Cloud NetApp Volumes storage pools, learn about system health, get the well-architected analysis for your systems, and explore savings.
2. Optional: Select **Operations and remediation** If you also want Workload Factory to manage Google Cloud NetApp Volumes resources and fix configuration issues.
3. Review the setup instructions at [Set up Google Cloud NetApp Volumes](#) before you continue.

Step 2: Create the Google Cloud service account

Steps

1. Expand **Set up your Google Cloud environment**.
2. Complete the steps 1-5 that are displayed to create a Google Cloud service account.
3. Copy the service account email address.
4. Return to Workload Factory, paste the email address into the **GCP service account** field, and select **Validate credentials**.
5. After validation is complete, from the **Projects** dropdown, select the Google Cloud project that you want Workload Factory to manage.
NOTE: The Projects list is unavailable until the service account credentials are verified.

Step 3: Enter the credentials name

Steps

1. Expand **Credentials name**.
2. In the **Name** field, enter a credentials name using only alphanumeric characters. Special characters and spaces are not allowed.
3. Select **Add**.

Result

The Google Cloud NetApp Volumes credentials are added to your account and are available for supported Workload Factory operations.

Configuration analysis for Google Cloud NetApp Volumes

The well-architected dashboard in NetApp Console analyzes storage system configurations regularly to determine if there are any configuration issues. 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 storage pool analysis, you must do the following:

- [Add your Google Cloud NetApp Volumes system to NetApp Console.](#)
- Grant *view, planning, and analysis* permissions in your Google Cloud account.

[Learn how to grant permissions to a Google Cloud account](#)

Best practices and recommendations for storage workloads

Workload Factory assesses storage configurations against storage and ONTAP best practices and the Google Cloud Well-Architected Framework. The assessment also recommends improvements.

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

Reliability

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

- **Snapshot policy**

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

- **SSD capacity headroom**

Workload Factory recommends keeping SSD tier usage at 80% or less. Some workloads may require additional capacity headroom and lower utilization targets. As usage exceeds the recommended headroom, the risk of performance slowdowns and service issues increases—especially if capacity isn't expanded in time. You can dismiss it for one or more storage pools and reactivate it later if needed.

Operational excellence

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

- **Volume capacity headroom**

Workload Factory recommends keeping volume usage under 80% to reduce the risk of running out of space. If a volume grows faster than expected, you might need to expand it quickly. This can increase the risk of application impact, especially with sudden or spiky growth. This risk is lower when you use thin provisioning and automatic capacity management. You can dismiss it for one or more volumes and reactivate it later if needed.

What's next

[Implement well-architected Google Cloud NetApp Volumes configurations](#)

Implement well-architected Google Cloud NetApp Volumes configurations

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

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

About this task

NetApp analyzes Google Cloud NetApp Volumes storage pool deployments in Google Cloud daily. The daily analysis provides the well-architected status, and insights and recommendations to help you understand configuration issues so that your storage pools meet best practices.

After the daily analysis completes, the dashboard displays the total number of well-architected resources, the number of resources in a critical state, and the number of resources in a warning state. Configurations are categorized by the pillars of the well-architected framework: reliability, operational excellence, cost optimization, performance efficiency, and security. The dashboard also includes a table that lists all configurations, the well-architected status of those configurations, the severity, category, resource type (volume or storage pool), impacted resources, and the option to view the recommendation when the configuration is not optimized.

Before you begin

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

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, download a CSV file of the recommendations for all configurations.

4. Review the recommendation.

Dismiss a configuration analysis

Stop a configuration analysis for a Google Cloud NetApp Volumes storage pool or for selected volumes. You can restart the analysis when needed.

Dismiss a configuration analysis for a storage pool

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.
4. Under Configurations, identify the configuration that doesn't apply to your environment and then select **Dismiss**.
5. 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. From the Well-architected dashboard, select **View** for any configuration.
4. Under Configurations, identify the configuration to dismiss for selected volumes and then select **View**.
5. 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.
6. Select **Dismiss** to stop the analysis for the configuration.
7. In the Dismiss volumes dialog, select **Dismiss** to confirm.

Result

The configuration analysis stops for the storage pool 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 storage pool

Steps

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

3. Select **Dismissed configurations**.
4. 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 system reactivates the configuration analysis. A new analysis occurs daily.

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.