



Set up Google Cloud

Project Astra

Ben Cammett, Erika Barcott
September 28, 2020

This PDF was generated from <https://docs.netapp.com/us-en/project-astra/get-started/set-up-google-cloud.html> on September 29, 2020. Always check docs.netapp.com for the latest.

Table of Contents

- Set up Google Cloud 1
 - Quick start 1
 - Create a service account that has the required permissions..... 2
 - Create a service account key 3
 - Enable APIs in your Google Cloud project 4
 - Enable private service access to Cloud Volumes Service for Google Cloud 4

Set up Google Cloud

A few steps are required to prepare your Google Cloud project before you can manage Google Kubernetes Engine clusters with the Project Astra beta program.

Quick start

Get started quickly by following these steps or scroll down to the remaining sections for full details.



Set up a Google Cloud account and project

You need a [Google Cloud account](#) and a [project](#).



Create a service account that has the required permissions

Create a [Google Cloud service account](#) that has the following permissions:

- Kubernetes Engine Admin
- NetApp Cloud Volumes Admin
- Storage Admin
- Service Usage Viewer
- Compute Network Viewer



Create a service account key

Create a [key for the service account](#) and save the key file in a secure location.



Enable APIs in your Google Cloud project

Enable the following [Google Cloud APIs](#):

- Google Kubernetes Engine
- Cloud Storage
- Cloud Storage JSON API
- Service Usage
- Cloud Resource Manager API
- NetApp Cloud Volumes Service

- Service Networking API
- Service Management API



Enable private service access to Cloud Volumes Service for Google Cloud

Set up private service access for [Cloud Volumes Service for Google Cloud](#).

The following image depicts the steps that you'll need to complete.

Create a service account that has the required permissions

Project Astra uses a Google Cloud service account to facilitate Kubernetes application data management on your behalf.

Steps

1. Go to Google Cloud and [create a service account by using the console, gcloud command, or another preferred method](#).
2. Grant the service account the following roles:
 - **Kubernetes Engine Admin** - Used to list clusters and create admin access to manage apps.
 - **NetApp Cloud Volumes Admin** - Used to manage persistent storage for apps.
 - **Storage Admin** - Used to manage buckets and objects for backups of apps.
 - **Service Usage Viewer** - Used to check if the required Cloud Volumes Service for Google Cloud APIs are enabled.
 - **Compute Network Viewer** - Used to check if the Kubernetes VPC is allowed to reach Cloud Volumes Service for Google Cloud.

The following video shows how to create the service account from the Google Cloud console.

▶ <https://docs.netapp.com/us-en/project-astra/get-started/media/video-create-gcp-service-account.mp4>

(video)

Create a service account key

Instead of providing a user name and password to Project Astra, you'll provide a service account key when you add your first cluster. Project Astra uses the service account key to establish the identity of the service account that you just set up.

The service account key is plaintext stored in the JavaScript Object Notation (JSON) format. It contains information about the GCP resources that you have permission to access.

You can only view or download the JSON file when you create the key. However, you can create a new key at any time.

Steps

1. Go to Google Cloud and [create a service account key by using the console, gcloud command, or another preferred method](#).
2. When prompted, save the service account key file in a secure location.

The following video shows how to create the service account key from the Google Cloud console.

► <https://docs.netapp.com/us-en/project-astra/get-started/media/video-create-gcp-service-account->

Enable APIs in your Google Cloud project

Your project needs permissions to access specific Google Cloud APIs. APIs are used to interact with Google Cloud resources, such as Google Kubernetes Engine (GKE) clusters and NetApp Cloud Volumes Service storage.

Step

1. Use the [Google Cloud console](#) or [gcloud CLI](#) to enable the following APIs:

- Google Kubernetes Engine
- Cloud Storage
- Cloud Storage JSON API
- Service Usage
- Cloud Resource Manager API
- NetApp Cloud Volumes Service
- Service Networking API
- Service Management API

The last two APIs are required for Cloud Volumes Service for Google Cloud.

The following video shows how to enable the APIs from the Google Cloud console.

► <https://docs.netapp.com/us-en/project-astra/get-started/media/video-enable-gcp-apis.mp4> (video)

Enable private service access to Cloud Volumes Service for Google Cloud

Project Astra uses Cloud Volumes Service for Google Cloud as the backend storage for your persistent volumes. Other than the APIs that you enabled in the previous step, the only other requirement is to enable private service access to Cloud Volumes Service.

Step

1. Set up private service access from your project to create a high-throughput and low-latency data-path connection, [as described in the Cloud Volumes Service for Google Cloud documentation](#).

Copyright Information

Copyright © 2020 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.

RESTRICTED RIGHTS LEGEND: Use, duplication, or disclosure by the government is subject to restrictions as set forth in subparagraph (c)(1)(ii) of the Rights in Technical Data and Computer Software clause at DFARS 252.277-7103 (October 1988) and FAR 52-227-19 (June 1987).

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.