



# Create a New Service Account (gcloud)

## Project Astra

Ben Cammett  
September 22, 2020

This PDF was generated from <https://docs.netapp.com/us-en/project-astra/get-started/gcp-create-service-account-gcloud.html> on October 18, 2020. Always check docs.netapp.com for the latest.

# Table of Contents

- Create a New Service Account (gcloud)..... 1
  - Set Your Project..... 1
  - Create a Service Account ..... 2
  - Add the Required Roles..... 2
  - Verify Roles ..... 3
  - Create a Key..... 4
- Next Steps..... 4

# Create a New Service Account (gcloud)

Learn how to create a new service account for your Google Cloud Platform account from the command line, using the `gcloud` tool.

For instructions on creating a new service account from the GCP console using a web browser, see [Create a New Service Account \(Browser\)](#).

## Requirements

- An active GCP account.
- A GCP project. [Create a New GCP Project](#).
- Google Cloud SDK (the `gcloud` tool) installed.

## External Resources

To install the Google Cloud SDK so that you can use the `gcloud` tool, see the official Google Cloud user guides:

- [Install Google Cloud SDK](#)
- [Set Up Google Cloud SDK](#)

To learn more about GCP service accounts, [see the official Google Cloud documentation](#).

## Set Your Project

Verify that your default `gcloud` configuration points to the project where you want to create the new service account:

```
gcloud config list
```

This command returns all of your GCP configurations:

```
jdoe@jdoe-laptop:~$ gcloud config list
[compute]
region = us-central1
zone = us-central1-c
[core]
account = jdoe@example.com
disable_usage_reporting = False
project = astra-sandbox

Your active configuration is: [default]
```

In this example, `astra-sandbox` is set as the GCP project.

To change the project, [follow the Google Cloud instructions for changing your default configuration](#).

## Create a Service Account

Create a name for your new service account.

- The name must be between 6 and 30 characters.
- It can contain upper- and lower-case alphanumeric characters and dashes, but no spaces or special characters.
- You can't change the service account name after you create it.
- The name is a unique identifier, which will appear in the service account's email address that Google creates, like `sa-name@project-id.iam.gserviceaccount.com`.

Set the new name as an environmental variable:

```
SA=[service account name]
```

For example, the command to set `example-service-account` is:

```
SA=example-service-account
```

Set the project ID as an environmental variable:

```
PROJECT_ID=`gcloud config list --format="text(core.project)" | awk '{print $NF}'`
```

Create the new service account:

```
gcloud iam service-accounts create ${SA}
```

## Add the Required Roles

If the policy role binding is set up with conditions, please select the correct condition from the list of conditions. If none of the conditions are required, select **None**.

### Compute Network Viewer

```
gcloud projects add-iam-policy-binding ${PROJECT_ID}
--member=serviceAccount:${SA}@${PROJECT_ID}.iam.gserviceaccount.com
--role=roles/compute.networkViewer
```

## Kubernetes Engine Admin

```
gcloud projects add-iam-policy-binding ${PROJECT_ID}
--member=serviceAccount:${SA}@${PROJECT_ID}.iam.gserviceaccount.com
--role=roles/container.admin
```

## Cloud Volumes Admin

```
gcloud projects add-iam-policy-binding ${PROJECT_ID}
--member=serviceAccount:${SA}@${PROJECT_ID}.iam.gserviceaccount.com
--role=roles/netappcloudvolumes.admin
```

## Storage Admin

```
gcloud projects add-iam-policy-binding ${PROJECT_ID}
--member=serviceAccount:${SA}@${PROJECT_ID}.iam.gserviceaccount.com
--role=roles/storage.admin
```

## Service Usage Viewer

```
gcloud projects add-iam-policy-binding ${PROJECT_ID}
--member=serviceAccount:${SA}@${PROJECT_ID}.iam.gserviceaccount.com
--role=roles/serviceusage.serviceUsageViewer
```

# Verify Roles

Check to make sure that all roles were added correctly.

```
gcloud projects get-iam-policy ${PROJECT_ID} --flatten="bindings[].members"
--format="table(bindings.role)"
--filter=bindings.members:${SA}@${PROJECT_ID}.iam.gserviceaccount.com
```

The output should match:

```
ROLE
roles/compute.networkViewer
roles/container.admin
roles/netappcloudvolumes.admin
roles/serviceusage.serviceUsageViewer
roles/storage.admin
```

## Create a Key

Create the service account JSON file:

```
gcloud iam service-accounts keys create ${SA}_keys.json --iam
-account=${SA}@${PROJECT_ID}.iam.gserviceaccount.com
```

This command creates a new file named `[service account name]_keys.json` in your current directory. In step one of the "Add Compute" wizard, you will be asked to upload this file to Project Astra.

## Next Steps

Now that you have created a service account and the JSON key file, you are ready to provision a new GKE cluster and add it to Project Astra. See our [Getting Started Guide](#) for instructions.

## 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.