<u>VPC Service Controls</u> (https://cloud.google.com/vpc-service-controls/) <u>Documentation</u> (https://cloud.google.com/vpc-service-controls/docs/) <u>Guides</u>

# Creating a service perimeter

This page describes how to create a service perimeter.

### Before you begin

- Read the <u>Overview of VPC Service Controls</u> (https://cloud.google.com/vpc-service-controls/docs/overview)
- Read about <u>configuring service perimeters</u> (https://cloud.google.com/vpc-service-controls/docs/service-perimeters)

### Creating a service perimeter

Note: Service perimeters cannot contain projects from different Organizations.

This section describes how to create a service perimeter that *does not* allow external access to services protected by the perimeter. If you want to create a service perimeter that permits limited external access, refer to Enabling controlled access when creating a perimeter (#external-access).

After you create a service perimeter, it may take up to 30 minutes for the changes to propagate and take effect.

CONSOLE GCLOUD API

1. In the Google Cloud Console navigation menu, click **Security**, and then click **VPC Service Controls**.

#### GO TO THE VPC SERVICE CONTROLS PAGE (HTTPS://CONSOLE.CLOUD.GOOGLE.COM/SECURITY/S

- 2. If you are prompted, select your Organization.
- 3. At the top of the VPC Service Controls page, click New Perimeter.
- 4. On the **New VPC Service Perimeter** page, in the **Perimeter Name** box, type a name for the perimeter.
- 5. Select the projects that you want to secure within the perimeter:
  - a. Click the **Add Projects** button.
  - b. In the **Add Projects** window, in each row corresponding to a project that you want add to the perimeter, select the checkbox.
  - c. Click the **Add** *n* **Projects** button, where *n* is the number of projects you selected in the previous step.

← New VPC	Service Perime	ter	
VPC Service Perime be part of the perim Perimeter Name Internal Corpu	Add project	cts elect will be secured within	your VPC Service Perimeter.
Must begin with a Perimeter Type Regular perim	<ul> <li>Filter pro</li> <li>Name</li> </ul>	ojects ₽ <b>↑</b>	<b>P</b> roject ID
O Perimeter brid Perimeter bridg	🗹 🐌 P2 C	ustomer Payments	coffee-shop-197323
Projects to protec	🗹 🐌 PA C	ustomer Accounts	numeric-amphora-193900
ADD PROJECTS	Rows per page:	andor Accounts	firewood-197323
Services to protect			CANCEL ADD 2 PROJECTS

- 6. Select the services that you want to secure within the perimeter:
  - a. Click the Add Services button.
  - b. In the **Specify services to restrict** window, in each row corresponding to a service that you want to protect, select the checkbox.
  - c. Click the **Add** *n* **Services** button, where *n* is the number of services you selected in the previous step.

VPC Service Perime be part of the perim Perimeter Name Internal Corpu Must begin with a	Specify services to restrict The services you restrict will be secured inside the service perimeter. Only services that fully support the VPC Service Perimeter are listed.
Perimeter Type	= Filter services
Regular service	
Perimeter bridg	BigQuery API
Projects to protec	Cloud Key Management Service (KMS) API ALPHA
Projec	Google Bigtable API
P2 Cu	Google Cloud Dataproc API
PA Cu	Google Cloud Pub/Sub API
ADD PROJECTS	Google Cloud Spanner API ALPHA
Services to protec	Google Cloud Storage API
Specify which servic controls can be add	Google Container Registry API ALPHA
restrict all storage s	Stackdriver Logging API

### Enabling controlled access when creating a perimeter

You can also apply one or more access levels when creating a new perimeter. If preferred, access levels can also be added <u>after a service perimeter is created</u>

(https://cloud.google.com/vpc-service-controls/docs/manage-service-perimeters # add-access-level).

After you create a service perimeter, it may take up to 30 minutes for the changes to propagate and take effect.

### Before you begin

Identify or <u>create access levels</u> (https://cloud.google.com/vpc-service-controls/docs/use-access-levels) that you want to apply to your service perimeters.

CONSOLE GCLOUD

1. In the Google Cloud Console navigation menu, click **Security**, and then click **VPC Service Controls**.

GO TO THE VPC SERVICE CONTROLS PAGE (HTTPS://CONSOLE.CLOUD.GOOGLE.COM/SECURITY/S

- 2. If you are prompted, select your Organization.
- 3. At the top of the **VPC Service Controls** page, click **New Perimeter**.
- 4. On the **New VPC Service Perimeter** page, in the **Perimeter Name** box, type a name for the perimeter.
- 5. Select the projects that you want to secure within the perimeter:
  - a. Click the Add Projects button.
  - b. In the **Add Projects** window, in each row corresponding to a project that you want add to the perimeter, select the checkbox.
  - c. Click the **Add** *n* **Projects** button, where *n* is the number of projects you selected in the previous step.



- 6. Select the services that you want to secure within the perimeter:
  - a. Click the Add Services button.
  - b. In the **Specify services to restrict** window, in each row corresponding to a service that you want to protect, select the checkbox.
  - c. Click the **Add** *n* **Services** button, where *n* is the number of services you selected in the previous step.

VDC Carulas Darim	
PC Service Perim be part of the perin Perimeter Name Internal Corp Must begin with	Specify services to restrict The services you restrict will be secured inside the service perimeter. Only services that fully support the VPC Service Perimeter are listed.
Perimeter Type <ul> <li>Regular perin</li> </ul>	= Filter services
Regular servic	
Perimeter brid	BigQuery API
Projects to prote	Cloud Key Management Service (KMS) API
Proje	Google Bigtable API
ۥ P2 C	Google Cloud Dataproc API
- PA C	Google Cloud Pub/Sub API
ADD PROJECT	Google Cloud Spanner API ALPHA
Services to prote	Google Cloud Storage API
Specify which serv	Google Container Registry API ALPHA
restrict all storage	s Stackdriver Logging API

- 7. Click the **Choose Access Level** box.
- 8. Select the checkboxes corresponding to the access levels that you want to apply to the service perimeter.
- 9. Click the **Save** button.

## What's next

 Learn how to <u>manage existing</u> (https://cloud.google.com/vpc-service-controls/docs/manage-service-perimeters) security perimeters. Except as otherwise noted, the content of this page is licensed under the <u>Creative Commons Attribution 4.0 License</u> (https://creativecommons.org/licenses/by/4.0/), and code samples are licensed under the <u>Apache 2.0 License</u> (https://www.apache.org/licenses/LICENSE-2.0). For details, see our <u>Site Policies</u> (https://developers.google.com/terms/site-policies). Java is a registered trademark of Oracle and/or its affiliates.

Last updated December 4, 2019.