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

# Supported products and limitations

This page contains a table of products and services that are supported by VPC Service Controls, as well as a list of known limitations with certain services and interfaces.

## Supported products

**Note:** This table includes *all* products that are supported by VPC Service Controls and function normally *inside* a service perimeter. However, not all supported products have services that can be directly protected by a service perimeter (#apis_and_service_perimeters).

VPC Service Controls supports the following products.

| Supported products | | |
|---|---|---|
| AI Platform Training (https://cloud.google.com/ml-engine/docs/) | **Details** | VPC Service Controls supports AI Platform Training online prediction), even though the two products sh |
| | **Limitations** | Known limitations (#aip-training) |
| Anthos Service Mesh (https://cloud.google.com/service-mesh/docs/) | **Details** | VPC Service Controls perimeters can only protect th perimeter to protect your Identity Namespace (https://cloud.google.com/kubernetes-engine/docs |
| BigQuery (https://cloud.google.com/bigquery/docs/) | **Details** | When you protect the BigQuery API using a service p to separately add the BigQuery Storage API to your |
| | **Limitations** | Known limitations (#bigquery) |

| Supported products | | |
|---|---|---|
| Cloud Bigtable (https://cloud.google.com/bigtable/docs/) | **Details** | None |
| Compute Engine (https://cloud.google.com/compute/docs/) | **Details** | VPC Service Controls support for Compute Engine e Kubernetes Engine private clusters inside service pe |
| | **Limitations** | Known limitations (#computeengine) |
| Dataflow (https://cloud.google.com/dataflow/docs/) | **Details** | Dataflow supports a number of storage service con following connectors have been verified to work wit<br>• Cloud Storage (Java (https://github.com/apache/beam/tree/maste , Python (https://github.com/apache/beam/bl<br>• BigQuery (Java, Python (https://beam.apache.<br>• Pub/Sub ( Java (https://github.com/apache/beam/tree/maste platform/src/main/java/org/apache/beam/sdk , Python (https://github.com/apache/beam/bl<br>• Cloud Bigtable (Java (https://github.com/apache/beam/tree/maste platform/src/main/java/org/apache/beam/sdk )<br>• Cloud Spanner (Java (https://github.com/apache/beam/tree/maste platform/src/main/java/org/apache/beam/sdk ) |
| | **Limitations** | Known limitations (#dataflow) |
| Dataproc (https://cloud.google.com/dataproc/docs/) | **Details** | Dataproc requires some special steps (https://cloud protect using VPC Service Controls. |
| | **Limitations** | Known limitations (#dataproc) |
| Cloud Data Loss Prevention (https://cloud.google.com/dlp/docs/) | **Details** | None |
| Cloud Key Management Service (https://cloud.google.com/kms/docs/) | **Details** | None |

| Supported products | | |
|---|---|---|
| Pub/Sub (https://cloud.google.com/pubsub/docs/) | **Details** | VPC Service Controls protection applies to all push a |
| | **Limitations** | Known limitations (#pubsub) |
| Cloud Spanner (https://cloud.google.com/spanner/docs/) | **Details** | None |
| Cloud Storage (https://cloud.google.com/storage/docs/) | **Details** | None |
| | **Limitations** | Known limitations (#storage) |
| Cloud SQL (https://cloud.google.com/sql/docs/) | **Details** | VPC Service Controls perimeters protect the Cloud S |
| | **Limitations** | Known limitations (#cloud_sql_admin_api) |
| Video Intelligence API (https://cloud.google.com/video-intelligence/docs/) | **Details** | None |
| Cloud Vision API (https://cloud.google.com/vision/docs/) | **Details** | None |
| Container Registry (https://cloud.google.com/container-registry/docs/) | **Details** | In addition to being able to protect the Container Re with GKE and Compute Engine. |
| | **Limitations** | Known limitations (#registry) |
| Google Kubernetes Engine (https://cloud.google.com/kubernetes-engine/docs/) | **Details** | None |
| Resource Manager (https://cloud.google.com/resource-manager/docs/) | **Details** | None |
| | **Limitations** | Known limitations (#crm) |
| Stackdriver Logging (https://cloud.google.com/logging/docs/) | **Details** | While VPC Service Controls protects most types of l resources. Because of this, Folder-level and Organiz information, refer to the known service limitations. |
| | **Limitations** | Known limitations (#logging) |
| Stackdriver Profiler (https://cloud.google.com/profiler/docs/) | **Details** | None |

| Supported products | | |
|---|---|---|
| Stackdriver Trace (https://cloud.google.com/trace/docs/) | **Details** | None |
| Cloud TPU (https://cloud.google.com/tpu/docs/) | **Details** | None |
| Natural Language API (https://cloud.google.com/natural-language/docs/) | **Details** | None |
| Cloud Asset API (https://cloud.google.com/asset-inventory/docs/) | **Details** | Because VPC Service Controls doesn't yet support F at the folder or organizational level is not protected service limitations. |
| | **Limitations** | Known limitations (#id) |
| Text-to-Speech (https://cloud.google.com/text-to-speech/docs/) | **Details** | None |

For more information, read about supported and unsupported services (https://cloud.google.com/vpc-service-controls/docs/troubleshooting#services).

## APIs and service perimeters

Not all products that are supported by VPC Service Controls have a service that can be protected by a service perimeter. Only the following APIs can be protected with a perimeter:

| APIs and service addresses | |
|---|---|
| AI Platform Training and Prediction API (#table_aip-training) BETA (https://cloud.google.com/products/#product-launch-stages) | ml.googleapis.com |
| BigQuery API (#table_bigquery) | bigquery.googleapis.com |
| Cloud Bigtable API (#table_bigtable) | bigtable.googleapis.com |
| Cloud Asset Inventory API (#table_cloudasset) | cloudasset.googleapis.com |
| Dataflow API (#table_dataflow) | dataflow.googleapis.com |

| APIs and service addresses | |
|---|---|
| Dataproc API (#table_dataproc) | dataproc.googleapis.com |
| Cloud Data Loss Prevention API (#table_dlp) BETA (https://cloud.google.com/products/#product-launch-stages) | dlp.googleapis.com |
| Cloud Key Management Service API (#table_kms) | cloudkms.googleapis.com |
| Cloud Natural Language API (#table_language) BETA (https://cloud.google.com/products/#product-launch-stages) | language.googleapis.com |
| Pub/Sub API (#table_pubsub) | pubsub.googleapis.com |
| Cloud Service Mesh Certificate Authority API (#table_asm) BETA (https://cloud.google.com/products/#product-launch-stages) | meshca.googleapis.com |
| Cloud Spanner API (#table_spanner) | spanner.googleapis.com |
| Cloud Storage API (#table_storage) | storage.googleapis.com |
| Cloud SQL API (#table_sql) | sqladmin.googleapis.com |
| Cloud Vision API (#table_vision) BETA (https://cloud.google.com/products/#product-launch-stages) | vision.googleapis.com |
| Container Registry API (#table_registry) | containerregistry.googleapis.com |
| Google Kubernetes Engine API (#table_gke) | container.googleapis.com |
| GKE Connect API (#table_gke) BETA (https://cloud.google.com/products/#product-launch-stages) | gkeconnect.googleapis.com |
| GKE Hub API (#table_gke) BETA (https://cloud.google.com/products/#product-launch-stages) | gkehub.googleapis.com |
| Resource Manager API (#table_crm) BETA (https://cloud.google.com/products/#product-launch-stages) | cloudresourcemanager.googleapis.com |
| Stackdriver Logging API (#table_logging) | logging.googleapis.com |
| Stackdriver Profiler API (#table_profiler) BETA (https://cloud.google.com/products/#product-launch-stages) | profiler.googleapis.com |
| Text-to-Speech API (#table_texttospeech) BETA (https://cloud.google.com/products/#product-launch-stages) | texttospeech.googleapis.com |

| APIs and service addresses | |
|---|---|
| Stackdriver Trace API (#table_trace) BETA (https://cloud.google.com/products/#product-launch-stages) | cloudtrace.googleapis.com |
| Cloud TPU API (#table_tpu) BETA (https://cloud.google.com/products/#product-launch-stages) | tpu.googleapis.com |
| Video Intelligence API (#table_videointelligence) BETA (https://cloud.google.com/products/#product-launch-stages) | videointelligence.googleapis.com |

## Unsupported services

**Warning:** While it may be possible to enable unsupported services to access the data of supported products and services, we recommend that you do not. Unexpected issues might occur when attempting to access a supported service using an unsupported service, especially within the same project.

Unsupported services may not function at all when enabled in a project protected by VPC Service Controls, especially when low-level storage services like Cloud Storage or Pub/Sub are restricted. We recommend deploying unsupported services in projects outside perimeters. To allow these services to access data in resources within a perimeter, create an access level (https://cloud.google.com/vpc-service-controls/docs/use-access-levels) that includes the service account for that service and apply it to perimeters as needed (https://cloud.google.com/vpc-service-controls/docs/manage-service-perimeters#add-access-level).

Attempting to restrict an unsupported service using the `gcloud` command-line tool or the Access Context Manager API will result in an error.

Cross-project access to data of supported services will be blocked by VPC Service Controls. Additionally, the restricted VIP can be used to block the ability of workloads to call unsupported services.

## Known limitations

This section describes known limitations with certain Google Cloud services, products, and interfaces that can be encountered when using VPC Service Controls.

For more information on resolving issues with VPC Service Controls, refer to the Troubleshooting (https://cloud.google.com/vpc-service-controls/docs/troubleshooting) page.

## AI Platform Training

- To fully protect your AI Platform Training training jobs, add all of the following APIs to the service perimeter:
  - AI Platform Training and Prediction API (`ml.googleapis.com`)
  - Pub/Sub API (`pubsub.googleapis.com`)
  - Cloud Storage API (`storage.googleapis.com`)
  - Google Kubernetes Engine API (`container.googleapis.com`)
  - Container Registry API (`containerregistry.googleapis.com`)
  - Stackdriver Logging API (`logging.googleapis.com`)

  Read more about setting up VPC Service Controls for AI Platform Training (https://cloud.google.com/ml-engine/docs/vpc-service-controls-training).
- Training with TPUs (https://cloud.google.com/ml-engine/docs/tensorflow/using-tpus) is not supported when you use AI Platform Training inside a service perimeter.
- When you protect the AI Platform Training and Prediction API by using a service perimeter, you only protect AI Platform Training, not AI Platform Prediction. However, some AI Platform Prediction functionality is disabled (https://cloud.google.com/ml-engine/docs/vpc-service-controls-training#prediction).

## App Engine

- App Engine (both standard environment and flexible environment) is not supported by VPC Service Controls. Do not include App Engine projects in service perimeters.

  However, it is possible to allow App Engine apps created in projects *outside* service perimeters to read and write data to protected services *inside* perimeters. To allow your app to access the data of protected services, create an access level (https://cloud.google.com/access-context-manager/docs/create-access-level#members-example) that includes the project's App Engine service account. This does not enable App Engine to be used inside service perimeters.

## BigQuery

- VPC Service Controls does not support copying BigQuery resources protected by a service perimeter to another organization. Access levels do not enable you to copy across organizations.

  To copy protected BigQuery resources to another organization, download the dataset (for example, as a CSV file), and then upload that file to the other organization.

- The BigQuery Data Transfer Service is supported only for the following services:
  - Campaign Manager
  - Google Ad Manager
  - Google Ads
  - Google Cloud Storage
  - Google Merchant Center
  - Google Play
  - YouTube
- The BigQuery Classic Web UI (https://cloud.google.com/bigquery/docs/bigquery-classic-ui) is not supported. A BigQuery instance protected by a service perimeter cannot be accessed with the BigQuery Classic Web UI.
- The third-party ODBC driver for BigQuery cannot currently be used with the restricted VIP.
- BigQuery audit log records do not always include all resources that were used when a request is made, due to the service internally processing access to multiple resources.
- When using a service account (https://cloud.google.com/access-context-manager/docs/create-access-level#members-example) to access a BigQuery instance protected by a service perimeter, the BigQuery job must be run within a project inside the perimeter. By default, the BigQuery client libraries will run jobs within the service account or user's project, causing the query to be rejected by VPC Service Controls.

## Client libraries

- The Java and Python client libraries for all supported services are fully supported for access using the restricted VIP. Support for others language is at Alpha stage (https://cloud.google.com/products/#product-launch-stages) and should be used for testing purposes only.

- Clients must use client libraries that have been updated as of November 1, 2018 or later.
- Service account keys or OAuth2 client metadata used by clients must be updated as of November 1, 2018 or later. Older clients using the token endpoint must change to the endpoint specified in newer key material/client metadata.

## Cloud Billing

- To allow Cloud Billing export to a Cloud Storage bucket or BigQuery instance in a project protected by a service perimeter, the user that is configuring the export should be added (https://cloud.google.com/access-context-manager/docs/create-access-level#members-example) temporarily to an access level for the perimeter.

## Cloud Build

- Cloud Build is not supported by VPC Service Controls. Do not use Cloud Build inside service perimeters.

  However, it is possible to allow Cloud Build in projects *outside* service perimeters to read and write data to protected services *inside* perimeters. To allow Cloud Build to access the data of protected services, create an access level (https://cloud.google.com/access-context-manager/docs/create-access-level#members-example) that includes the project's Cloud Build service account. This does not enable Cloud Build to be used inside service perimeters.

## Cloud Composer

- Cloud Composer is not supported by VPC Service Controls. Do not use Cloud Composer inside service perimeters.

  To allow Cloud Composer to access resources inside a service perimeter, enable Cloud Composer in a project outside any service perimeter. Then, create and apply an access level to the perimeter that allows requests from the service account for your Cloud Composer environment.

## Dataflow

- Custom BIND and the `restricted.googleapis.com` VIP cannot be used for Dataflow (https://cloud.google.com/dataflow/docs/guides/routes-firewall#dns_limitations) because DNS resolution of Dataflow can't be customized.
- Not all storage service connectors have been verified to work when used with Dataflow inside a service perimeter. For a list of verified connectors, see the Dataflow details (#table_dataflow).

## Dataproc

- To protect a Dataproc cluster with a service perimeter, you must follow the instructions for setting up private connectivity (https://cloud.google.com/vpc-service-controls/docs/set-up-private-connectivity) to allow the cluster to function inside the perimeter.
- Cloud Dataproc Component Gateway (https://cloud.google.com/dataproc/docs/concepts/accessing/dataproc-gateways) does not support VPC Service Controls.

## Cloud Functions

- Cloud Functions is not supported by VPC Service Controls. Do not include Cloud Functions projects in service perimeters.

  However, it is possible to allow functions created in projects that are *outside* of your service perimeters to read and write data to protected services *inside* a perimeter. To allow your function to access the data of protected services, create an access level (https://cloud.google.com/access-context-manager/docs/create-access-level#members-example) that includes the project's Cloud Functions service account. This does not enable Cloud Functions to be used inside service perimeters.
- Functions cannot be created for a project in a perimeter that protects the Cloud Storage service.

## Pub/Sub

- Pub/Sub push subscriptions created prior to the service perimeter will not be blocked.

## Cloud Shell

- Cloud Shell is not supported. It is treated as outside of service perimeters and denied access to data protected by VPC Service Controls.

## Cloud Storage

- When using the Requester Pays feature (https://cloud.google.com/storage/docs/requester-pays) with a storage bucket *inside* a service perimeter that protects the Cloud Storage service, you cannot identify a project to pay that is *outside* the perimeter. The target project must be in the same perimeter as the storage bucket or in a perimeter bridge with the bucket's project.

  For more information about Requester Pays, see the Requester Pays use and access requirements (https://cloud.google.com/storage/docs/requester-pays#requirements).
- For projects in a service perimeter, the Cloud Storage page in the Cloud Console is not accessible if the Cloud Storage API is protected by that perimeter. If you want to grant access to the page, you must create an access level that includes either the user accounts or a public IP range that you want to allow to access the Cloud Storage API.
- In audit log records, the `resourceName` field does not identify the project that owns a bucket. The project must be discovered separately (https://cloud.google.com/vpc-service-controls/docs/troubleshooting#dataproc_example).
- In audit log records, the value for `methodName` is not always correct. We recommend that you do *not* filter Cloud Storage audit log records by `methodName`.
- In certain cases, Cloud Storage legacy bucket logs can be written to destinations outside of a service perimeter even when access is denied.
- When you attempt to use `gsutil` for the first time in a new project, you may be prompted to enable the `storage-api.googleapis.com` service. While you cannot directly protect `storage-api.googleapis.com`, when you protect the Cloud Storage API using a service perimeter, `gsutil` operations are also protected.

## Compute Engine

- Currently, you cannot protect the Compute Engine API using a service perimeter.
- To enable creating a Compute Engine image from a Cloud Storage in a project protected by a service perimeter, the user that is creating the image should be added (https://cloud.google.com/access-context-manager/docs/create-access-level#members-example) temporarily to an access level for the perimeter.

- Using Kubernetes with Compute Engine inside a service perimeter is not supported by VPC Service Controls.

## Container Registry

- Because it is not using the `googleapis.com` domain, Container Registry must be configured via Private DNS or BIND to map to the restricted VIP separately from other APIs.
- In addition to the containers inside a perimeter that are available to Container Registry, the following read-only Google-managed repositories are available to all projects regardless of service perimeters:
  - gcr.io/asci-toolchain
  - gcr.io/cloud-airflow-releaser
  - gcr.io/cloud-builders
  - gcr.io/cloud-dataflow
  - gcr.io/cloud-marketplace
  - gcr.io/cloud-ssa
  - gcr.io/cloudsql-docker
  - gcr.io/config-management-release
  - gcr.io/foundry-dev
  - gcr.io/fn-img
  - gcr.io/gke-node-images
  - gcr.io/gke-release
  - gcr.io/google-containers
  - gcr.io/kubeflow
  - gcr.io/kubeflow-images-public
  - gcr.io/kubernetes-helm
  - gcr.io/istio-release
  - gcr.io/ml-pipeline
  - gcr.io/projectcalico-org

- gcr.io/rbe-containers
- gcr.io/rbe-windows-test-images
- gcr.io/speckle-umbrella
- gcr.io/stackdriver-agents
- gcr.io/tensorflow
- gke.gcr.io
- k8s.gcr.io
- mirror.gcr.io

In all cases, the regional versions of these repositories are also available.

## Google Cloud Console

- Because the Cloud Console is only accessible over the internet, it is treated as outside of service perimeters. When you apply a service perimeter, the Cloud Console interface for the services that you protected may become partially or fully inaccessible. For example, if you protected Logging with the perimeter, you will not be able to access the Logging interface in the Cloud Console.

  To allow access from the Cloud Console to resources protected by a perimeter, you need to create an access level for a public IP range that includes the machines of users who want to use the Cloud Console with protected APIs. For example, you could add the public IP range of the NAT gateway of your private network to an access level, and then assign that access level to the service perimeter.

  If you want to limit Cloud Console access to the perimeter to only a specific set of users, you can also add those users to an access level. In that case, only the specified users would be able to access the Cloud Console.

## Resource Manager

- The only Resource Manager API methods that are protected are v1 `project.setIAMPolicy` (https://cloud.google.com/resource-manager/reference/rest/v1/projects/setIamPolicy) and v1beta1 `project.setIAMPolicy` (https://cloud.google.com/resource-manager/reference/rest/v1beta1/projects/setIamPolicy).

## Stackdriver Logging

- Aggregated export sinks (folder or organization sinks where `includeChildren` is `true`) can access data from projects inside a service perimeter. We recommend that Cloud IAM is used to manage Logging permissions at the folder and organization level.
- Because VPC Service Controls does not currently support folder and organization resources, log exports of folder-level and organization-level logs (including aggregate logs) do not support service perimeters. We recommend that Cloud IAM is used to restrict exports to the service accounts required to interact with the perimeter-protected services.
- To set up an organization or folder log export to a resource protected by a service perimeter, you must add the service account for that log sink to an access level and then assign it to the destination service perimeter. This is not necessary for project-level log exports.

  For more information, refer to the following pages:

  - Granting access from the internet with access levels (https://cloud.google.com/vpc-service-controls/docs/use-access-levels)
  - Managing service perimeters (https://cloud.google.com/vpc-service-controls/docs/manage-service-perimeters)
  - Overview of Logs Exports (https://cloud.google.com/logging/docs/export)

## Stackdriver Monitoring

- While Monitoring can sometimes be used with projects protected by a service perimeter, Monitoring is not officially supported by VPC Service Controls.

## Cloud Asset API

- When calling Cloud Asset API at the Folder or Organization level, data from projects inside a service perimeter that belongs to the folder or organization can still be accessed. We recommend that Cloud IAM is used to manage Cloud Asset Inventory permissions at the folder and organization level.

## Cloud SQL

- Service perimeters protect only the Cloud SQL Admin API. They do not protect IP-based data access to Cloud SQL instances. You need to use an organization policy constraint (https://cloud.google.com/sql/docs/mysql/configure-org-policy#configuring_the_organization_policy) to restrict public IP access on Cloud SQL instances.
- Cloud SQL imports and exports can only perform reads and writes from a Cloud Storage bucket within the same service perimeter as the Cloud SQL replica instance. In the external server migration flow (https://cloud.google.com/sql/docs/mysql/replication/replication-from-external#process), you need to add the Cloud Storage bucket to the same service perimeter. When creating a key flow for CMEK, you need to create the key (https://cloud.google.com/sql/docs/mysql/configure-cmek#key) in the same service perimeter as the resources that use it. Note: When restoring an instance from a backup, the target instance need to reside in the same service perimeter as the backup.

*Last updated January 3, 2020.*