Enhance security with VPC Service Controls

Google Cloud Search supports VPC Service Controls to enhance the security of your data. VPC Service Controls allows you to define a service perimeter around Google Cloud Platform resources to constrain data and help mitigate data exfiltration risks.

Note: Cloud Search supports restricted VIP which provides a private network route to make data and resources inaccessible from the internet. For information on setting up restricted VIP, refer to Setting up private connectivity to Google APIs and services (https://cloud.google.com/vpc-service-controls/docs/set-up-private-connectivity).

Prerequisites

Before you begin, install the gcloud command-line interface (https://cloud.google.com/sdk/gcloud).

Enable VPC Service Controls

To enable VPC Service Controls:

1. Obtain the project IDs and project numbers for the Google Cloud Platform project you want to use. To obtain the project IDs and numbers, refer to Identifying projects (https://cloud.google.com/resource-manager/docs/creating-managing-projects#identifying_projects).
2. Use gcloud to create an access policy for your Google Cloud Platform organization:
    a. Get your organization ID (https://cloud.google.com/resource-manager/docs/creating-managing-organization#retrieving_your_organization_id).
    b. Create an access policy (https://cloud.google.com/access-context-manager/docs/create-access-policy).

c. Get the name of your access policy (https://cloud.google.com/access-context-manager/docs/manage-access-policy#gcloud).

★ **Note:** Organizations can only have one access policy. If you attempt to create a second access policy for for your organization, an error occurs.

3. Create a service perimeter with Cloud Search as a restricted service by running the following gcloud command:

```
gcloud access-context-manager perimeters create NAME \
    --title=TITLE \
    --resources=PROJECTS \
    --restricted-services=RESTRICTED-SERVICES \
    --policy=POLICY_NAME
```

Where:

- `NAME` is the name of the perimeter.
- `TITLE` is the human-readable title of the perimeter.
- `PROJECTS` is a comma-separated list of one or more project numbers, each preceded by the string `projects/`. Use the project numbers obtained in step 1. For example, if you had two projects, project `12345` and `67890`, your setting would be `--resource=projects/12345, project/67890` .This flag only supports project numbers; it doesn't support names or IDs.
- `RESTRICTED-SERVICES` is a comma-separated list of one or more services. Use `cloudsearch.googleapis.com`.
- `POLICY_NAME` is the numeric name of your organization's access policy obtained in step 2c.

For further information on how to create a service perimeter, refer to Creating a service perimeter (https://cloud.google.com/vpc-service-controls/docs/create-service-perimeters).

4. (optional) If you want to apply IP or region-based restrictions, create access levels and add them to the service perimeter created in step 3:

a. To create an access level, refer to Creating an basic access level (https://cloud.google.com/access-context-manager/docs/create-basic-access-level). For

an example on how to create an access level condition that only allows access from a specific range of IP addresses, such as those within a corporate network, refer to Limit access on a corporate network (https://cloud.google.com/access-context-manager/docs/create-basic-access-level#corporate-network-example) .

b. After you have created an access level, add it to the service perimeter. For instructions on adding an access level to a service perimeter, refer to Adding an access level to an existing perimeter (https://cloud.google.com/vpc-service-controls/docs/manage-service-perimeters#add-access-level) . This change can take up to 30 minutes for this change to propagate and take effect.

5. Use the Cloud Search Customer Service REST API to update the customer settings with your VPC Service Controls perimeter-protected project:

Note: Because Cloud Search resources are not stored in a Google Cloud Platform project, you must update the Cloud Search customer settings with the VPC Service Controls perimeter-protected project. The VPC Service Controls project acts as a virtual project container for all your Cloud Search resources. Without building this mapping, VPC Service Controls won't work for the Cloud Search API.

1. Obtain an OAuth 2.0 access token from the Google Authorization Server. For information on obtaining the token, refer to step 2 of Using OAuth 2.0 to Access Google APIs (https://developers.google.com/identity/protocols/oauth2). When obtaining the access token, use one of the following OAuth scopes: `https://www.googleapis.com/auth/cloud_search.settings.indexing`, `https://www.googleapis.com/auth/cloud_search.settings`, or `https://www.googleapis.com/auth/cloud_search`
2. Run the following curl command to set the project in VPC Service Controls settings under Customer settings in Google Cloud Search:

```
curl --request PATCH \
  'https://cloudsearch.googleapis.com/v1/settings/customer' \
  --header 'Authorization: Bearer [YOUR_ACCESS_TOKEN]' \
  --header 'Accept: application/json' \
  --header 'Content-Type: application/json' \
  --data '{ "vpc_settings": { "project": "projects/PROJECT_ID" } }' \
  --compressed
```

Where:

- `YOUR_ACCESS_TOKEN` is OAuth 2.0 access token obtained in step 5a.
- `PROJECT_ID` is the project ID obtained in step 1.

If successful, you should receive a `200 OK` response accompanied by the updated customer settings.

After the above steps are completed successfully, the VPC Service Controls restrictions, as defined in the service perimeter, are applied to all Google Cloud Search APIs, searches at `cloudsearch.google.com`, and viewing and changing configuration or reports using the Admin console. Further requests to the Cloud Search REST API that don't follow access levels receive a `PERMISSION_DENIED "Request is prohibited by organization's policy"` error.

Last updated 2022-09-13 UTC.