# Agentless Install

Prepare your environment, then follow the wizard's prompts to install agentless Cloud Security Posture Management (CSPM), Identity and Access Management (CIEM), and Cloud Detection and Response (CDR) on GCP. You can connect single projects or organizations.

## Prerequisites

### Installed Applications

- Sysdig Secure SaaS with `administrator` permissions
- Terraform must be installed on the machine from which you will deploy the installation code, along with:
  - Terraform Google Platform Provider
  - Google's Cloud SDK must be deployed in the environment where you will deploy the installation code.

    For further guidance, see the Hashicorp and Google documentation: Install Terraform; Google Platform Provider; Install the gcloud CLI.
- Have on hand:
  - For Organizations: The GCP Organization domain, Organization Member Project ID, and Region
  - For Projects: The Project ID

## Review GCP Roles and Permissions

Review these concepts before preparing your environment and running the onboarding wizard.

Note that to assign user roles, enable APIs, and configure domain-wide delegation, you will need to log in to and access two different GCP consoles at different times:

- Google Cloud Console
- Google Admin Console

The steps are detailed in Prepare Your Environment and Configure Domain-Wide-Delegation.

## User Types

If you install by hand or on your local machine, you will want likely to install as a **user**. If you are automating the installation, such as using Terraform Cloud, you will likely want to install as a **service account**.

You can:

- Use an existing user or service account that meets the permissions requirements
- Create a new user or service account and set up permissions
- Add permissions to an existing user or service account

## Permissions Required to Install

### Single Project

The installing user/service account must have the following roles assigned on the Project that is being onboarded:

- `roles/iam.serviceAccountCreator`
- `roles/iam.roleAdmin`
- `roles/resourcemanager.projectIamAdmin`

If you are installing CDR, you must have the following **additional** roles assigned on the Project that is being onboarded:

- `roles/pubsub.editor`
- `roles/logging.configWriter`

### Organization

Note: Certain roles are required at the organization level. Other roles are required on a single project in which you will deploy shared resources. Ensure you have the correct roles assigned at the correct scope.

The installing user/service account must have the following roles assigned:

- `roles/iam.serviceAccountCreator` (On the project where shared resources will be created)
- `roles/iam.organizationRoleAdmin` (At the Organization level)
- `roles/resourcemanager.organizationAdmin` (At the Organization level)

If you are installing CDR, you must have the following **additional** roles assigned:

- `roles/pubsub.editor` (On the project where shared resources will be created)

- `roles/logging.configWriter` (On the project where shared resources will be created)

### Permissions Granted to Sysdig

The installation also creates a service account that Sysdig can access. This service account will be granted the following roles:

- `roles/browser`
- `roles/cloudasset.viewer`
- `roles/iam.serviceAccountTokenCreator`
- `roles/logging.viewer`
- `roles/recommender.viewer`
- `roles/iam.serviceAccountViewer`
- `roles/iam.roleViewer`
- `roles/container.clusterViewer`
- `roles/compute.viewer`

## Prepare Your Environment

Preparation of your GCP environment, roles, and permissions is the key to a seamless connection between your GCP cloud accounts and Sysdig. When preparation is complete, the installation itself is a simple, wizard-guided process from the Sysdig Secure UI.

Follow each of the steps below to prepare for onboarding.

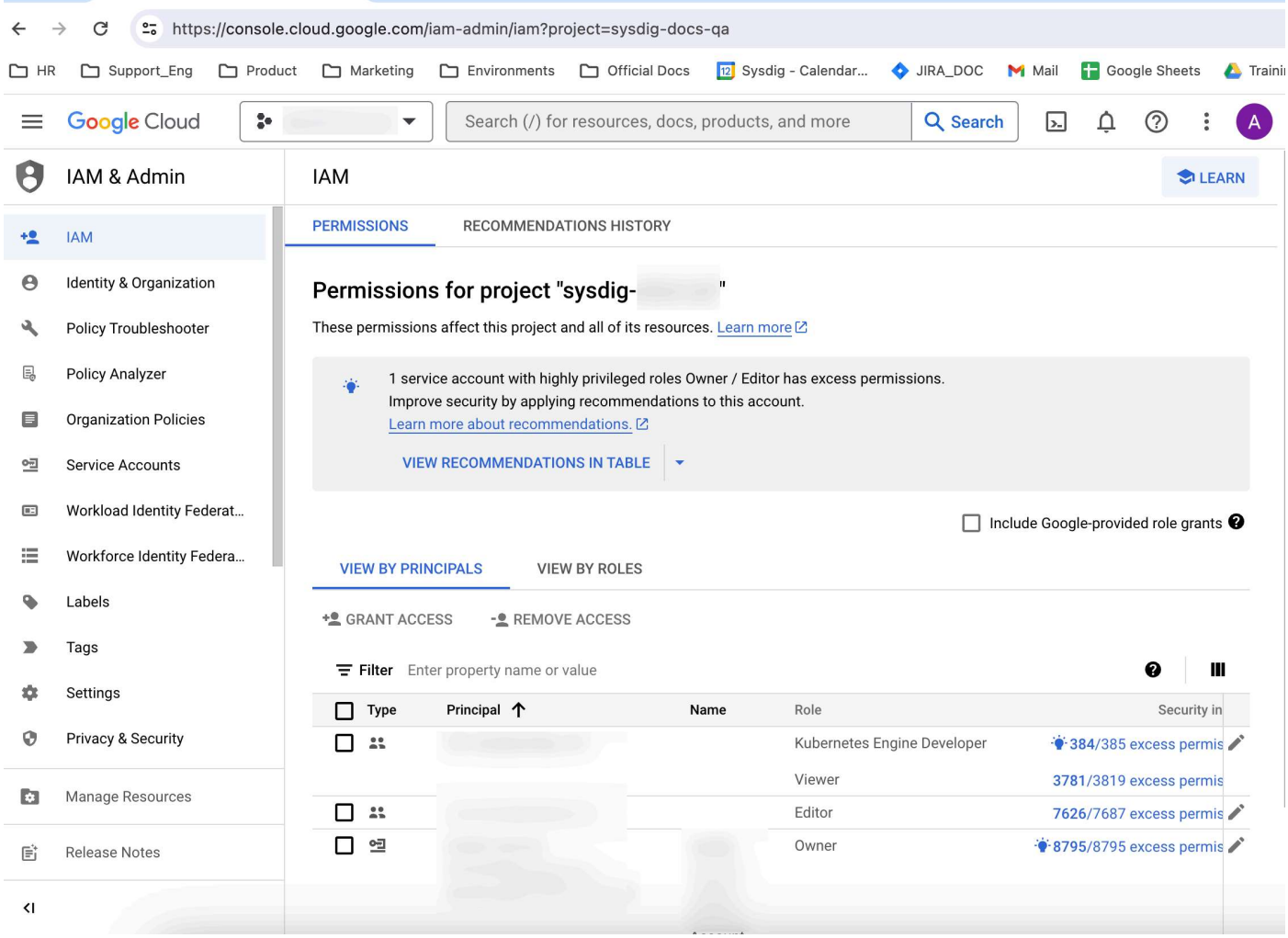
### Step 1: Provide User with Appropriate Roles

Ensure your user has the correct roles and permissions in GCP to perform the onboarding.

#### Single Project

To check or assign roles:

1. Log in to the Google Cloud Console as either a user or a service account, ensuring you have the correct project active.
2. Navigate to **IAM & Admin > IAM**.
3. In **VIEW BY PRINCIPALS**, find your User/service account.
4. Ensure that all the roles listed in Permissions Required to Install are present.
5. If any roles are missing, select your user/service account, and grant the roles using the **Grant Access** button. You may need to work with your administrator to be granted the correct roles.




### Organization

NOTE: Certain roles are required at the organization level. Certain roles are required on a single project in which you will deploy shared resources. Ensure you have the correct roles assigned at the correct scope.

For roles required on a single project, follow the instructions for a single project above.

For roles that are required at the organization level:

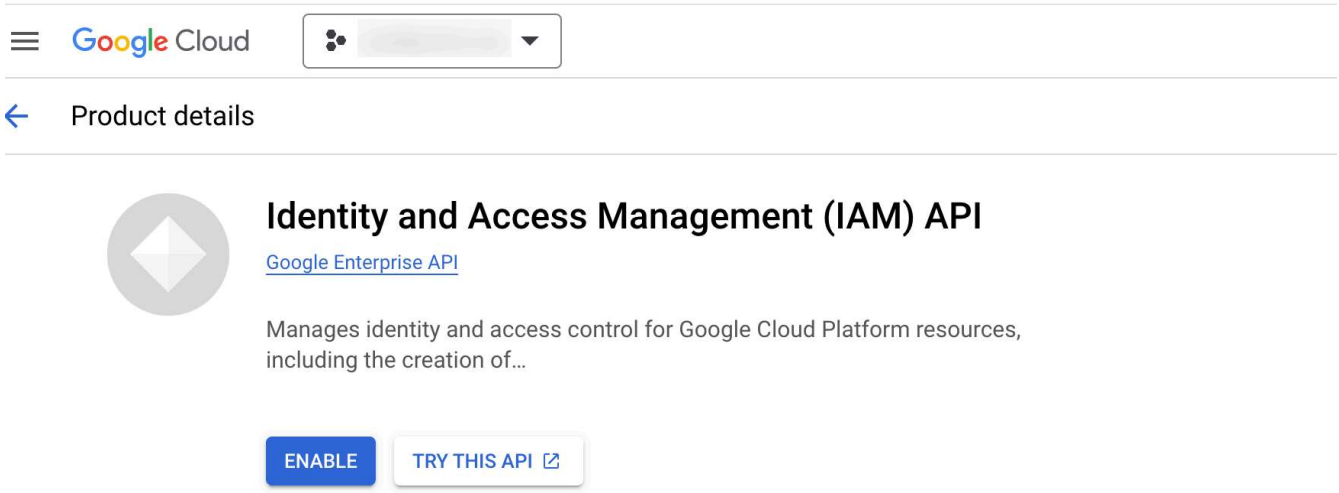
1. Log in to the Google Cloud Console as either a user or a service account.
2. Ensure the organization is selected in the project selector in the top bar. If you do not see your organization there, you may need to work with your administrator.
3. In **VIEW BY PRINCIPALS**, find your User/Super Administrator.
4. Ensure that all the roles listed in Permissions Required to Install are present.
5. If any roles are missing, select your user/service account, and grant the roles using the **Grant Access** button. You may need to work with your administrator to be granted the correct roles.

## Step 2: Enable Required APIs

The APIs must be enabled at the project level.

To do so manually:

1. Click each of the API links in the table below.
2. Select the appropriate project and click **Enable**.




| API Name | Used For | Which Project(s) |
|---|---|---|
| Identity and access management API (`iam.googleapis.com`) | All | All |
| IAM Service Account Credentials API (`iamcredentials.googleapis.com`) | All | All |
| Cloud Resource Manager API (`cloudresourcemanager.googleapis.com`) | All | All |
| Security Token Service API (`sts.googleapis.com`) | CSPM/CIEM | All |
| Recommender API (`recommender.googleapis.com`) | CSPM/CIEM | All |
| Cloud Identity API (`cloudidentity.googleapis.com`) | CSPM/CIEM | All |
| Admin SDK API (`admin.googleapis.com`) | CSPM/CIEM | All |
| Cloud Asset API (`cloudasset.googleapis.com`) | CSPM/CIEM | All |
| Cloud Pub/Sub API (`pubsub.googleapis.com`) | CDR | Project containing shared resources |

## Check API Enablement

To confirm that the required APIs were enabled:

1. Enable the `serviceusage.googleapis.com` Service API.

This is required to execute the following command.

2. Execute: `gcloud services list --enabled`

All the services listed above should be included.

### Step 3: Authenticate and Configure Terraform

Configure your environment from your local machine, preparing to apply Terraform.

1. Ensure the prerequisites are met:
   - Terraform v.1.3.1+ installed
   - gcloud CLI installed
2. Authenticate your user and configure Terraform to use these credentials.

   A common way to do this is:

   1. Ensure you are logged in to the correct project.

      Log in using the GCP CLI:

      ```
      gcloud auth application-default login
      ```

      You will be presented with a web page to select your user account. Be sure to log in as the user you configured in Step 1.

   2. Confirm you are logged in as the correct user, by running the following and confirming that the expected user is active:

      ```
      gcloud auth list
      ```

For assistance, or instructions on alternative ways to authenticate Terraform, see the Terraform documentation: Google Provider Configuration Reference.

## Install using Wizard

1. Ensure you are authenticated to the GCP project you would like to connect to in your terminal window. You can authenticate using the GCP CLI by running:

   `gcloud auth application-default login`.

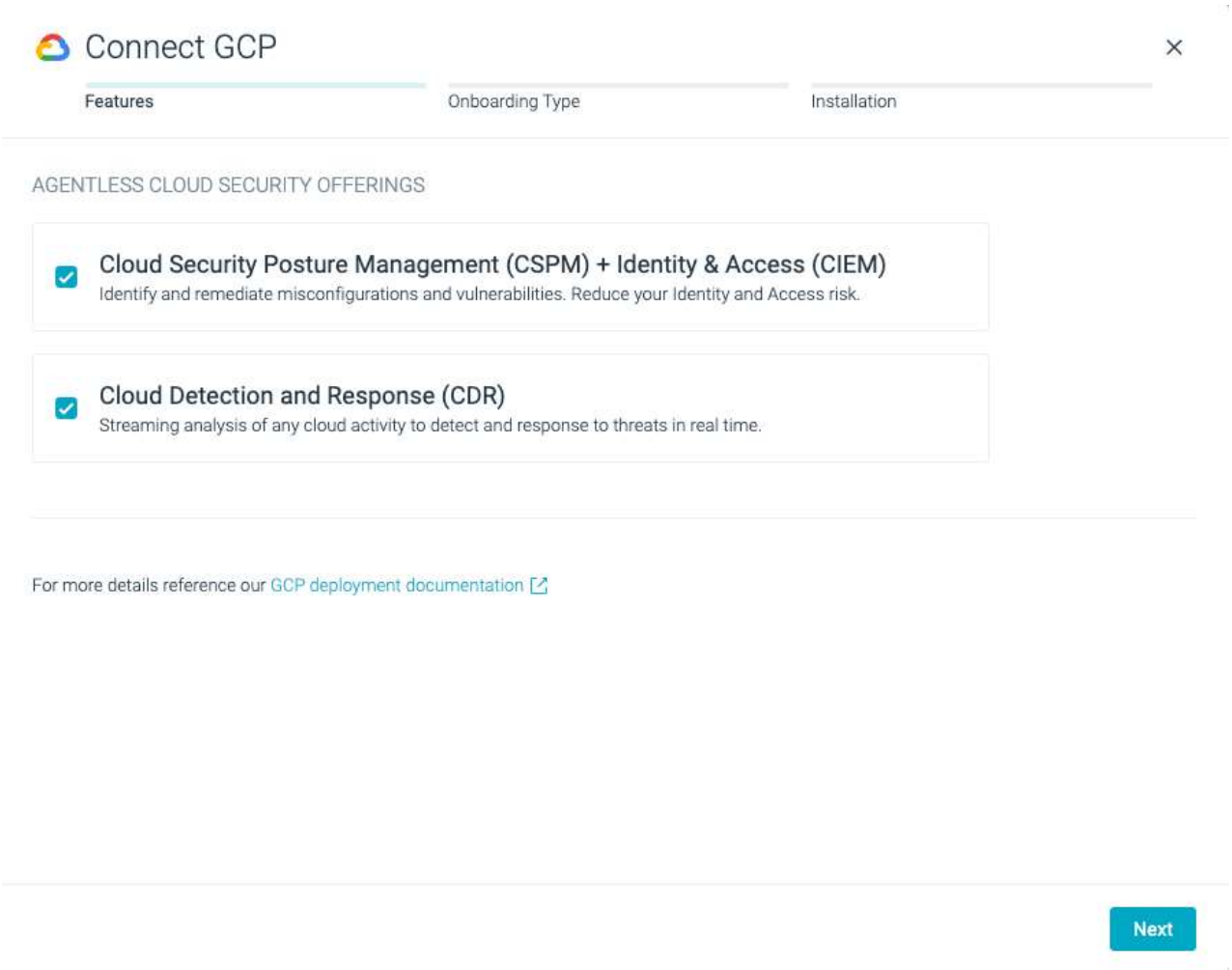
2. Log in to Sysdig Secure as `admin` and select **Integrations > Data Sources|Cloud Accounts**.

3. Click **+Add Account** and select **GCP**.

4. Choose which Agentless option you want:

   - **CSPM and CIEM**
   - **CDR** only
   - **All** together

   and click **Next**.




5. Select which installation method matches your enterprise and click **Next**.

   - **Organization:** Configure GCP for an Organization
   - **Project:** Configure GCP for a single Project account

The **Installation** screen appears.

## Installation

The entries on this page differ slightly depending on whether it's an Organization or Project installation.

### Organization

1. As prompted by the wizard screen, specify the following:
   - **Organization Domain:** The domain of the GCP organization you are onboarding.
   - **Region of your GCP Project:** The region where resources will be created in your GCP project.
   - **Project ID:** The GCP project where the Sysdig resources will be deployed.

   The wizard will auto-populate a code snippet, along with autodetected Sysdig Secure endpoint and Sysdig Secure API token information.
2. Run `terraform init && terraform apply`.
3. (CSPM+CIEM only): Click **Next** in the wizard to set up Domain-Wide Delegation in the Google Cloud Admin Console. Enabling DWD is optional and can be omitted if you don't want to provide those permissions to Sysdig.
4. After deploying, validate the services are working.

### Project

1. As prompted by the wizard screen, specify the following:
   - **Region of your GCP Project:** The region where resources will be created in your GCP project.
   - **Project ID:** The ID of the GCP project that you are onboarding.

   The wizard will auto-populate a code snippet, along with autodetected Sysdig Secure endpoint and Sysdig Secure API token information.
2. Run `terraform init && terraform apply`.
3. (CSPM+CIEM only): Click **Next** in the wizard to set up Domain-Wide Delegation in the Google Cloud Admin Console. Enabling DWD is optional and can be omitted if you don't want to provide those permissions to Sysdig.
4. After deploying, validate the services are working.

## Configure Domain-Wide Delegation

### What Is Domain-Wide-Delegation

In GCP, domain-wide delegation (DWD) refers to a feature in Google Workspace (formerly G Suite). It allows a Google Workspace super admin to delegate authority to a service account to access user data on behalf of users within the domain. Once set up, Sysdig uses a service account that can impersonate users by specifying the subject parameter in its authentication request, setting it to the email address of the Google Workspace user it wishes to impersonate.

Domain-wide delegation entails:

- **Service Account Access**: It allows a service account to impersonate a Google Workspace user and gain access to the Google data the user has access to, assuming they have provisioned the

necessary Authorization scopes to the Service Account.

- **No User Consent Required**: With DWD, individual user consent is not required. Once the super admin sets up the delegation, the service account can access the specified data of any user in the domain without additional authorization prompts.
- **OAuth 2.0 Scopes**: When setting up DWD, the super admin specifies which OAuth 2.0 scopes the service account is granted. For instance, they might grant access to the Directory API to allow the service account to read group member data.
- **Security**: Because DWD grants broad access, it's essential to handle it with care. The service account's private key, which is used for authentication, should be kept secure.

### Where it is Used

Sysdig's CIEM analysis requires DWD to provide:

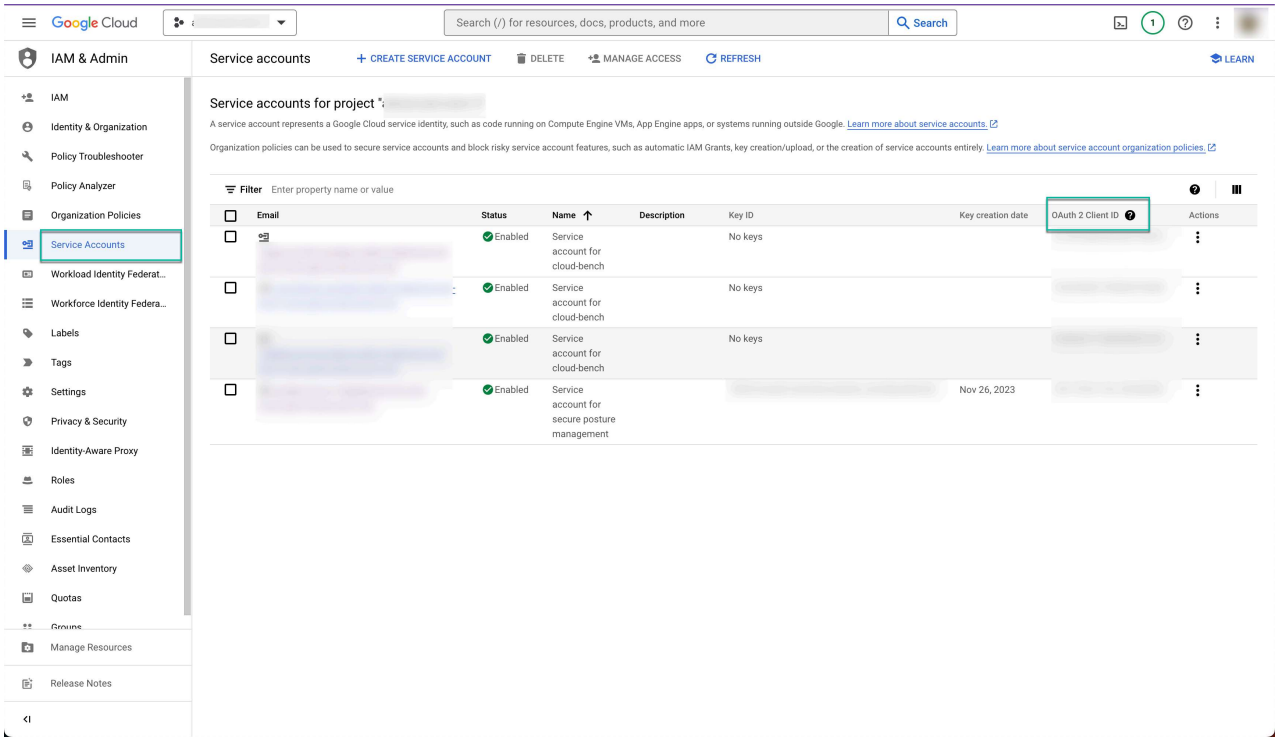
- User and Group Insights derived from Google Workspace and Cloud Identity If DWD is enabled, then *Actionable Risk*, *Excessive Permissions*, and *Members* are displayed on the Identity and Access Groups page.
- Enhanced Monitoring and Reporting for MFA usage, user logins, admin console changes, and third-party application access
- Asset management to gain insights into Roles, Service Accounts, and their associated keys

The onboarding wizard prompts you to perform domain-wide delegation. If you skip this step, you will be prompted again from the **Identity and Access** (CIEM) page of the Sysdig Secure UI.

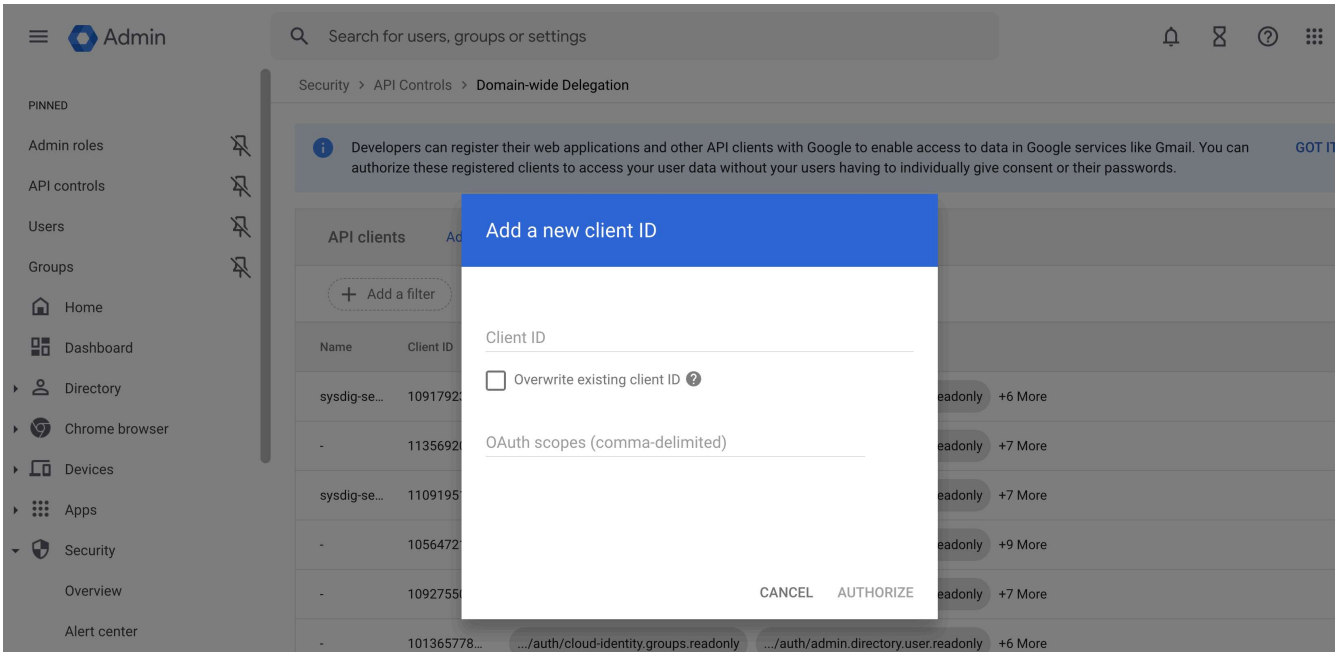
### Enable Domain-Wide Delegation in GCP

#### Authorize Service Account Scopes

1. Log in to the Google Admin Console with Super Administrator privileges and select **Security > Access and data control > API controls**.
2. Click **Manage Domain Wide Delegation**.
3. Click **Add New**.
4. Switch to the Google Cloud Console to collect your service account's **OAuth 2 Client ID**:
    - Navigate to the **Project** specified during the initial onboarding step.
    - Select **Service Account** and search for the newly created Sysdig service account with the format: `sysdig-secure-a1b2@your-project-id.iam.gserviceaccount.com`.
    - Click the **Service Account** link to display the **OAuth 2 Client ID** and copy it.




5. Return to the Google Admin Console from Step 3. (**Security > Access and data control > API controls > Manage Domain Wide Delegation > Add New** ).




In the panel, enter:

- **Client ID:** Paste the OAuth 2 Client ID you copied.
- **OAuth Scopes:** Add the OAuth scopes below in a comma-delimited list.

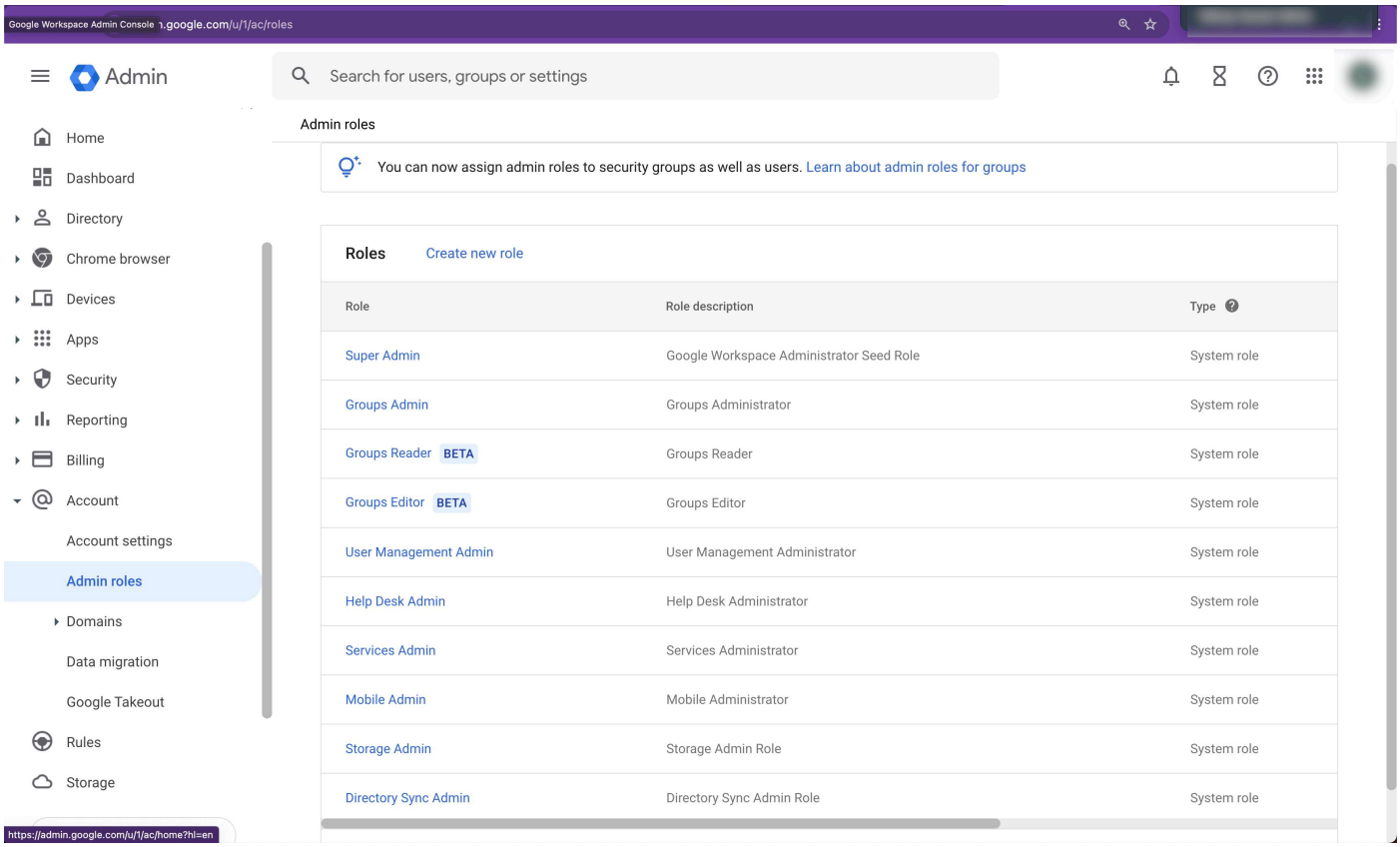
```
https://www.googleapis.com/auth/cloud-identity.groups.readonly,
https://www.googleapis.com/auth/admin.directory.user.readonly,
https://www.googleapis.com/auth/admin.directory.group.readonly,
https://www.googleapis.com/auth/admin.directory.group.member.readonly,
https://www.googleapis.com/auth/cloud-platform.read-only,
https://www.googleapis.com/auth/logging.read,
```

```
https://www.googleapis.com/auth/admin.reports.audit.readonly,
https://www.googleapis.com/auth/admin.reports.usage.readonly,
```

6. Click **Authorize**.

## Create a Custom Admin Role and Grant Privileges

While still in the Google Admin Console, go to **Account > Admin Roles**.

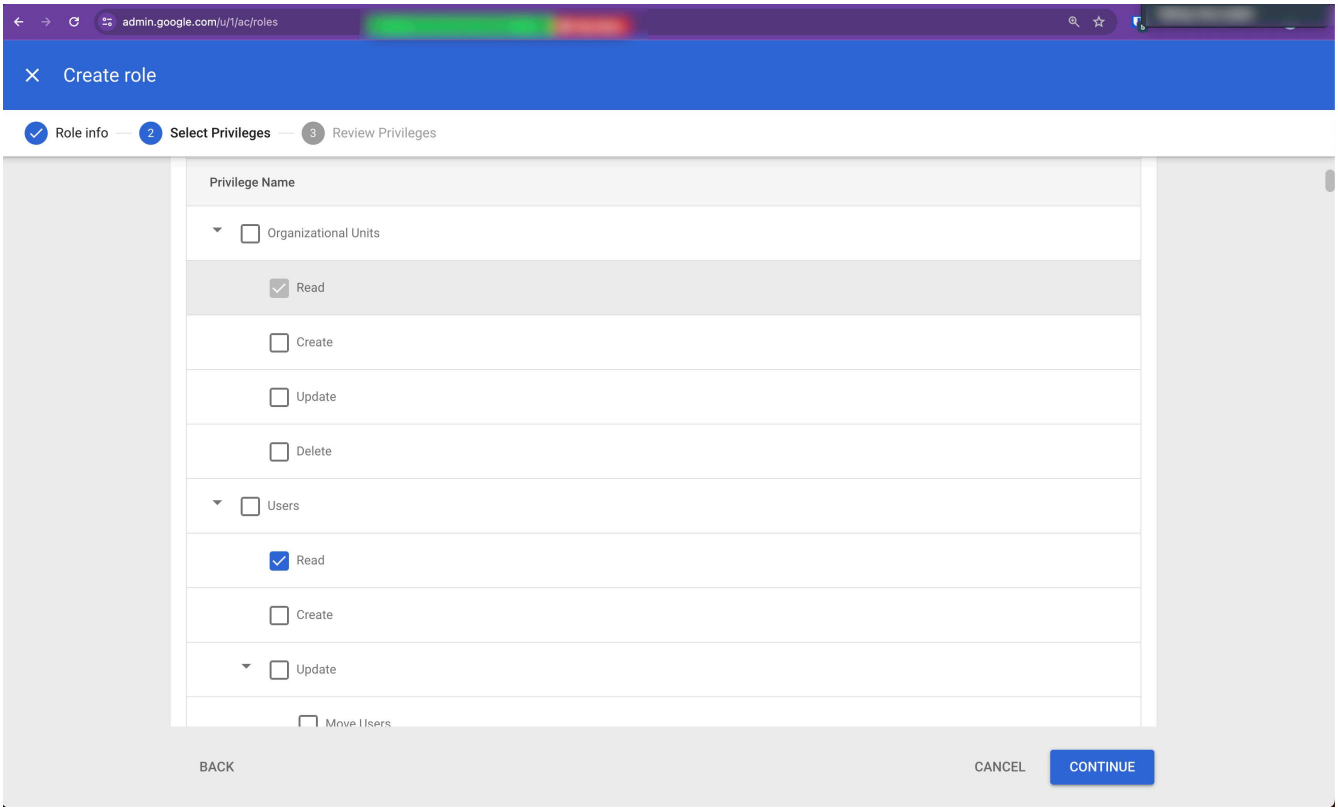



7. Click **Create new role**.

8. Enter the following values:

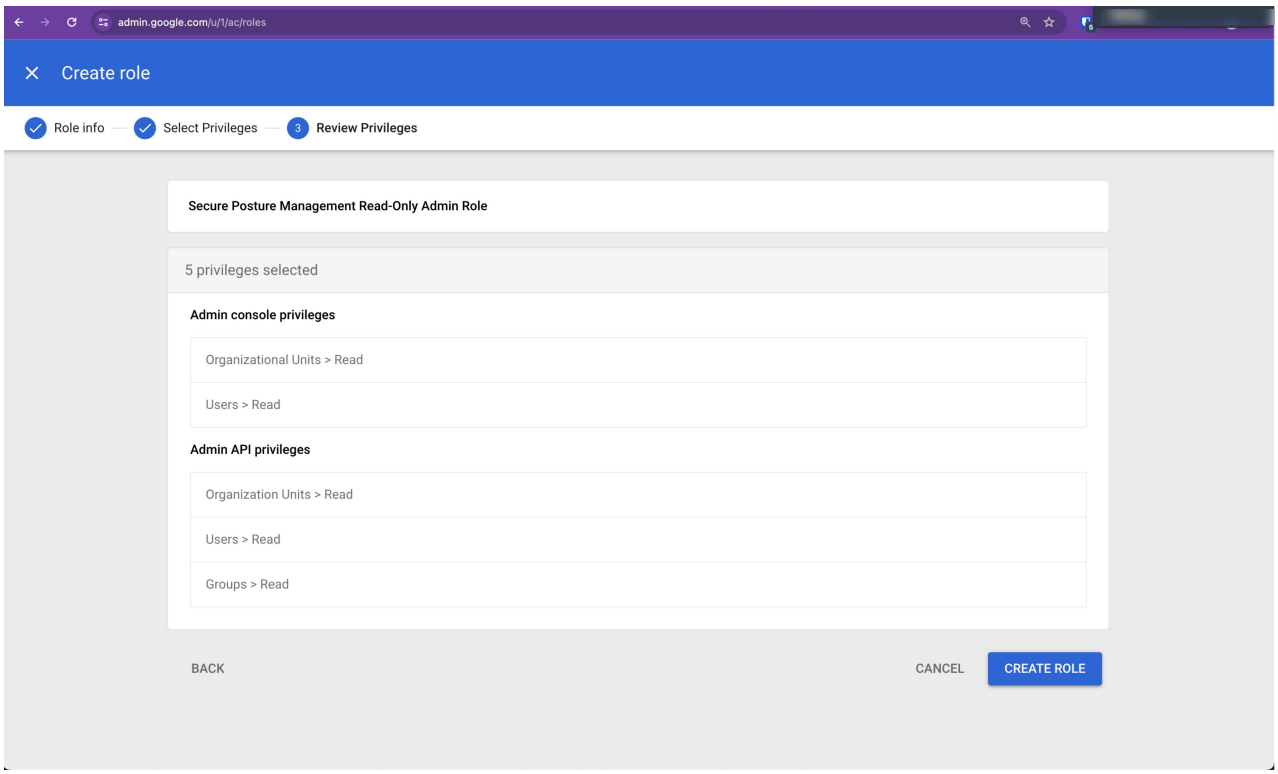
   - **Name:** Enter an appropriate name, such as `Secure Posture Management Read-Only Admin Role`.
   - **Description:** Optional

9. Click **Continue**. The **Select Privileges** page appears.

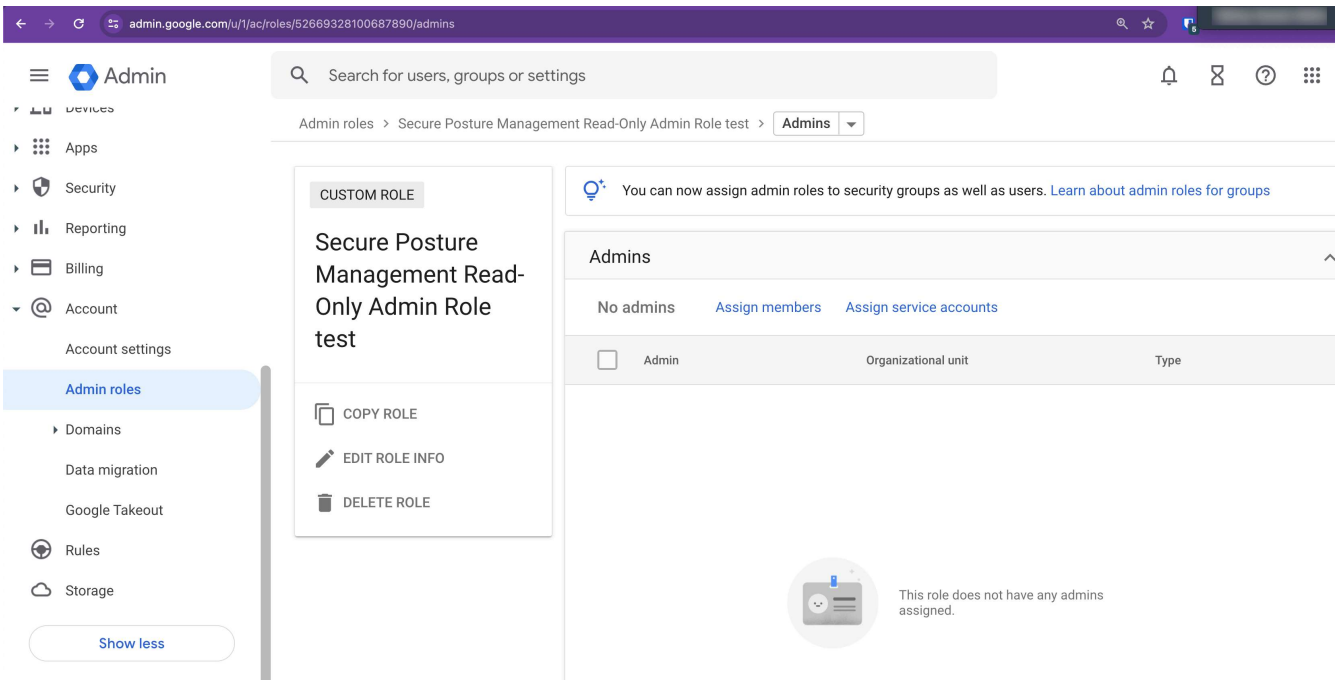



10. Configure the Select Privileges as follows:

    - In **Admin Console Privileges**, at the top of the page, enable:
        - `Organization Units - Read`
        - `Users - Read`
    - Scroll down to **Admin API Privileges** and enable:
        - `Groups - Read`
    - Click **Continue**. Confirm the 5 privileges.



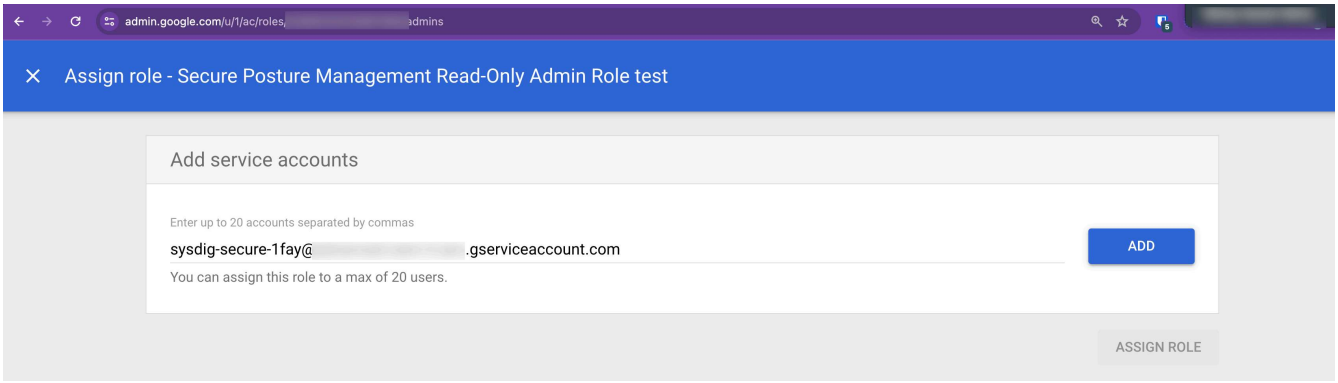
- Click **Create Role**. The **Admin Roles** screen appears.




11. Click **Assign Service Accounts**.

12. Enter the Sysdig service account name from step 4 and click **Add**.

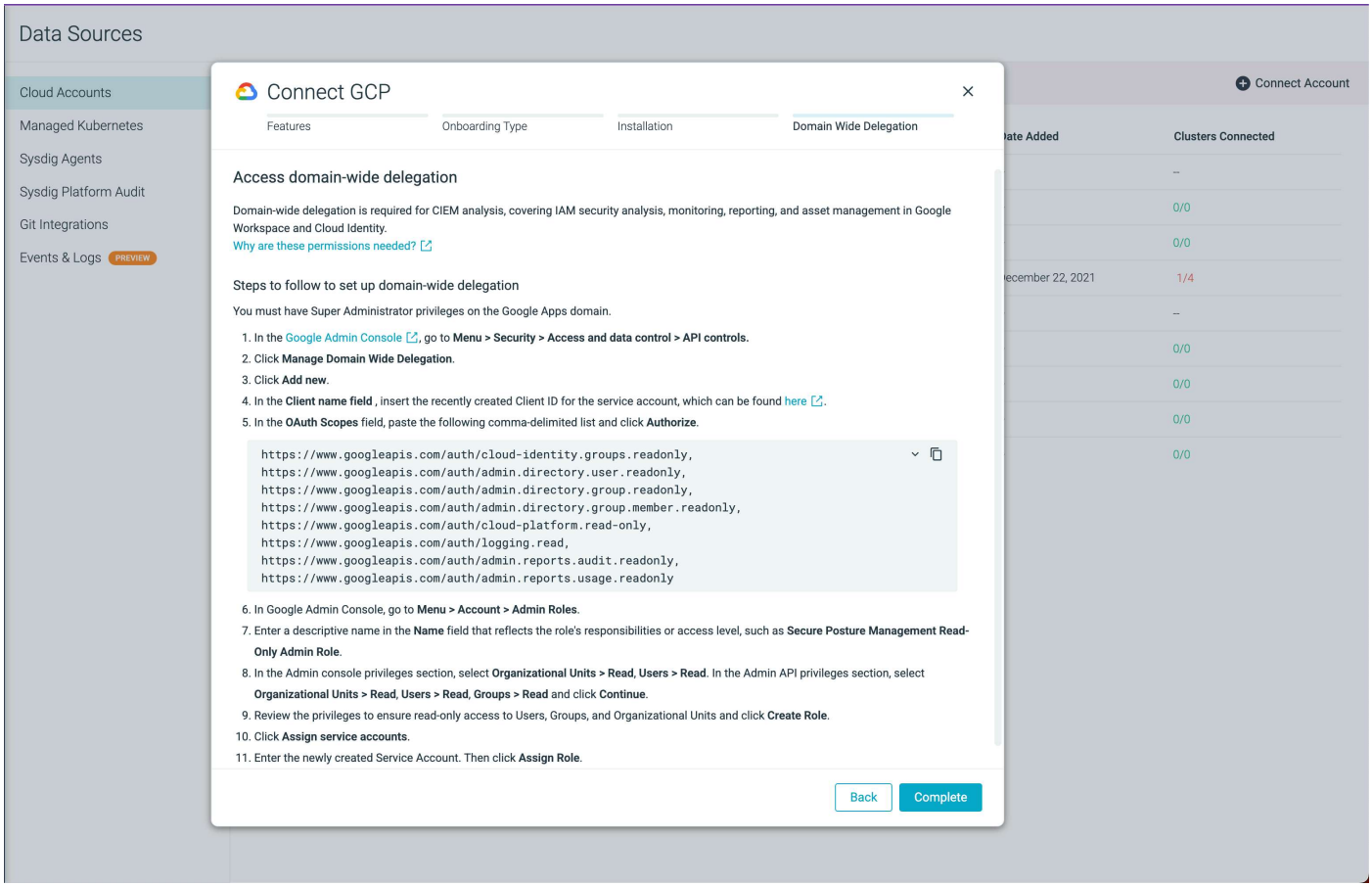
    (Format: `sysdig-secure-a1b2@your-project-id.iam.gserviceaccount.com`)




13. A confirmation screen is displayed; click **Assign Role**.

## Complete the Sysdig Onboarding Wizard

When all the enablement steps in GCP consoles are complete, return to the Sysdig wizard and click **Complete**.




# Validate

Log in to Sysdig Secure and check that each module you deployed is functioning. It may take 10 minutes or so for events to be collected and displayed.

## Check Overall Connection Status

**Data Sources:** Select **Integrations > Data Sources | Cloud Accounts** to see all connected cloud accounts.

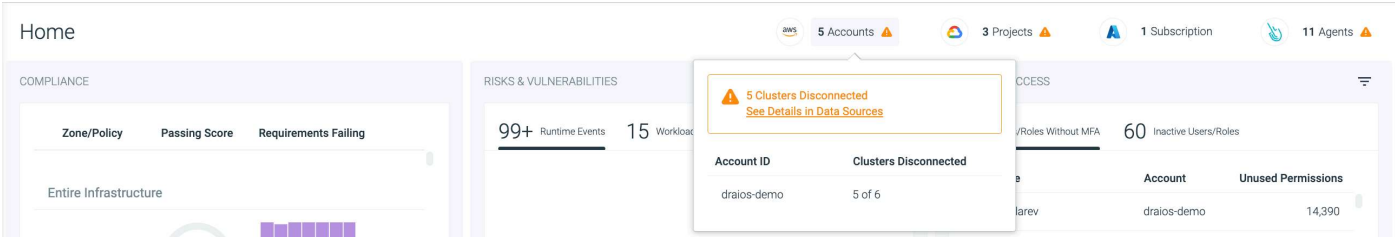
## Check CSPM

**Inventory:** Select the **Inventory** module and filter for `project =`. Check for your GCP cloud account in the drop-down.

## Check Identity and Access CIEM (Preview)

**Home:** Select **Home** and check the status bar at the top right to see your cloud accounts.

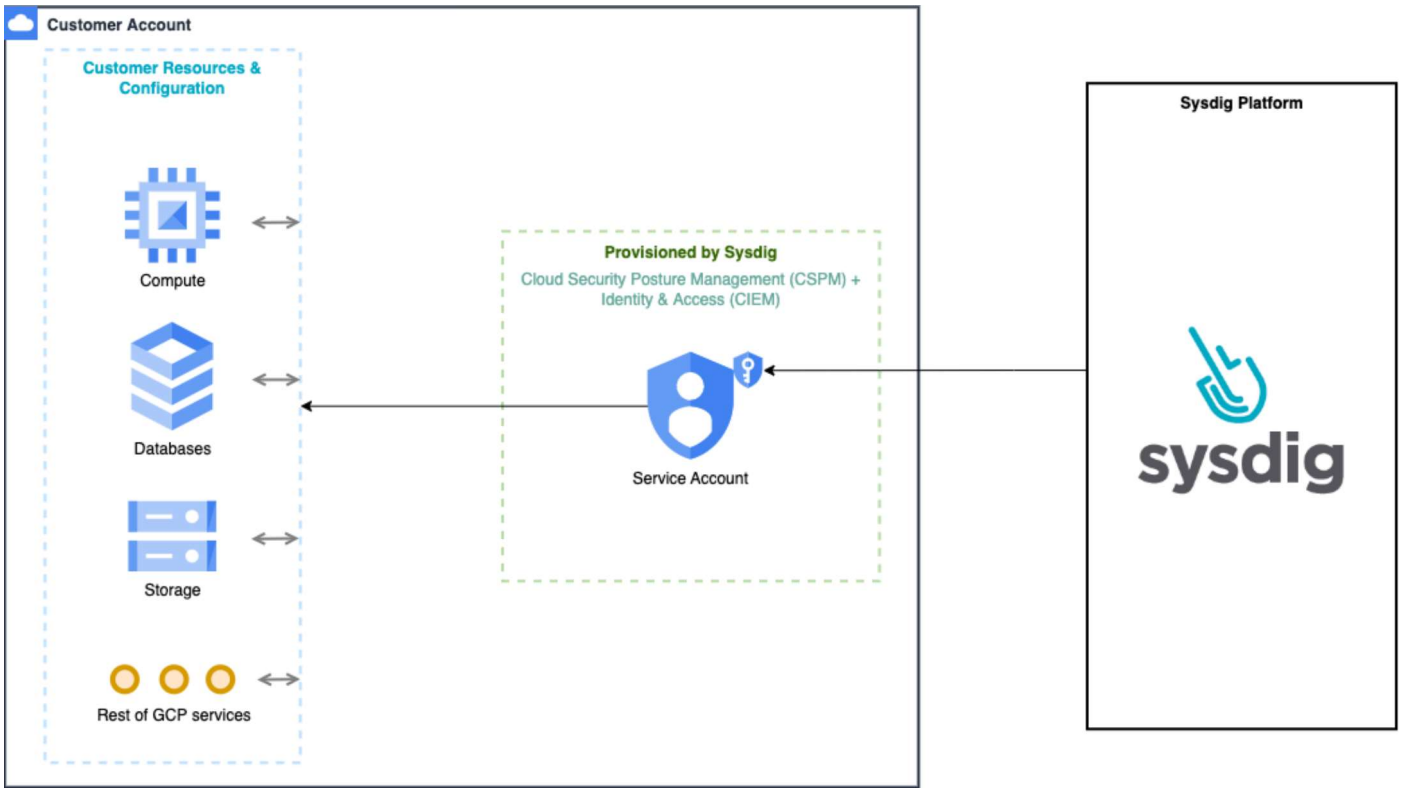
GCP resources are being rolled out for Identity and Access pages, starting with **Groups** page.




# Features and Resources on GCP

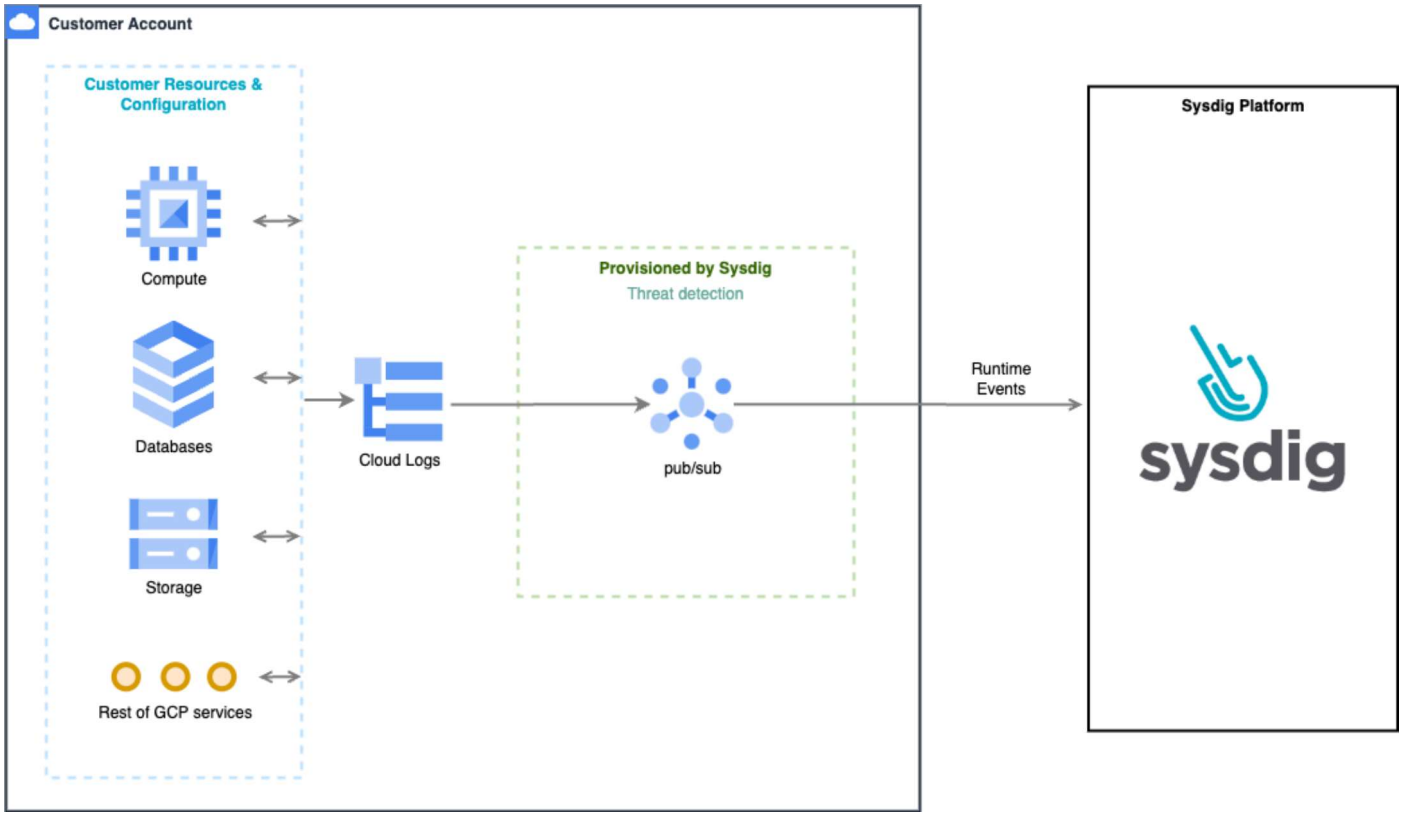
## Agentless CSPM and Agentless CIEM

### Resources Created




- `google_service_account`
- `google_service_account_key`
- `google_project_iam_member`
- `google_organization_iam_member` (Organizational Installs only)

## Agentless CDR




## Resources Created

- `google_service_account`
- `google_service_account_iam_binding`
- `google_pubsub_topic`
- `google_pubsub_subscription`
- `google_pubsub_topic_iam_member`
- `google_project_iam_audit_config` (Single project installs only)
- `google_organization_iam_audit_config` (Organizational Installs only)
- `google_logging_project_sink` (Single project installs only)
- `google_logging_organization_sink` (Organizational Installs only)