Any application programs that use Google Cloud resources need a Google Cloud identity and permissions before they can access the resources.

On Google Cloud, Cloud Identity and Access Management (Cloud IAM) uses *service accounts* to establish identities for programs and *roles* to grant permissions to the service accounts of the programs.

For SAP systems and related programs that run on Compute Engine virtual machines (VMs), create a VM service account that contains only the roles that the SAP systems and other programs need.

Programs that do not run on Google Cloud can use service accounts when they connect to Google Cloud APIs and use a service account key for authentication.

Programs that run on a Compute Engine VM can use the service account of the VM, as long as the VM service account has the roles the program needs. For programs that are running on a Compute Engine VM, using a service account key for authentication is not recommended.

When you create a VM instance using the `gcloud` command-line tool or the Google Cloud Console (https://console.cloud.google.com/), you can specify a service account for the VM instance to use, accept the project default service account, or specify no service account.

When you create an instance by making a request to the API directly without using the `gcloud` command-line tool or the Google Cloud Console, the default service account does not come enabled with the instance.

If a VM service account doesn't have the roles the program needs, you can add roles to the VM service account or replace the service account with a new VM service account.

The Compute Engine default service account for a project is initially granted the Editor role (/iam/docs/understanding-roles#primitive_role_definitions), which might be too permissive for many enterprise environments.

For more information about the use of roles, permissions, and service accounts by Compute Engine, see:

- Service accounts (/compute/docs/access/service-accounts)
- Creating and enabling service accounts for instances (/compute/docs/access/create-enable-service-accounts-for-instances)

For information that applies more broadly across Google Cloud, see the Cloud IAM documentation:

- Cloud IAM overview (/iam/docs/overview)
- Understanding roles (/iam/docs/understanding-roles)
- Understanding service accounts (/iam/docs/understanding-service-accounts)

If you are deploying your SAP infrastructure by using the Deployment Manager templates that are provided by Google Cloud, you can specify a VM service account in the `template.yaml` configuration file.

If you do not specify a service account, Deployment Manager deploys the VMs with the default service account of your project.

Cloud IAM provides predefined roles for each Google Cloud resource. Each role contains a set of permissions for the resource that are appropriate to the level of the role. You can add these roles to the service accounts that you create.

For the most restrictive or granular control, you can create custom roles with one or more permissions.

For a list of the predefined roles and the permissions that each contains, see Understanding roles (/iam/docs/understanding-roles#predefined_roles).

For more information about custom roles, see Understanding custom roles (/iam/docs/understanding-custom-roles).

For more information about roles that are specific to Compute Engine, see Compute Engine Cloud IAM roles (/compute/docs/access/iam) in the Compute Engine documentation.

The Cloud IAM roles that your SAP programs need depends on the resources that the programs use and on the tasks that the programs perform.

For example, if you use Cloud Deployment Manager to deploy your SAP system and specify a service account in the Deployment Manager configuration file, the service account that you specify must include at least the following roles:

- Service Account User - always required.
- Compute Instance Admin - always required.
- Storage Object Viewer - required to download installation media from a Cloud Storage bucket during deployment.
- Logs Writer - required to write deployment or other messages to Logging.

After the SAP system deploys, the host VM and your SAP programs might not need all of the same permissions that were required during deployment. You can edit the VM service account to remove roles, or change the service account that the VM uses.

Some SAP or related programs require additional roles and, if they are not running on Google Cloud, might require a separate service account. For example:

- The Cloud Storage Backint agent for SAP HANA (/solutions/sap/docs/sap-hana-backint-guide) requires the Storage Object Admin role to back up to and recover from Cloud Storage.
- The SAP HANA Monitoring agent requires you to install Stackdriver Monitoring agents, which require the Monitoring Metric Writer role. For more information, see Setting the required Cloud IAM roles (/solutions/sap/docs/sap-hana-monitoring-agent-user-guide#setting_the_required_iam_roles).
- SAP Data Services, when it is configured to replicate SAP data to BigQuery (/solutions/sap/docs/bigquery-replication-from-sap-apps), requires both the BigQuery Data Editor role and the BigQuery Job User role.