# Installing a cluster on GCP into an existing VPC - Required GCP Permissions

***Disclaimer:*** *The audience of this document will consider any information provided by Red Hat Support in reference to the case#03001508 official. The information below does not supersede that provided by Red Hat Support.* ***THIS DOCUMENT SPECIFICALLY CREATED FOR IBM. NOT TO BE DISTRIBUTED TO THE CUSTOMER CVS****.*

**Objective:** The purpose of this document is to attempt to provide some context into the elevated privilege roles needed by the service account user account in a gcp (Google Cloud Platform) project within the gcp environment for a successful installation of OpenShift Container Platform. The roles that will be discussed below are only project level roles, meaning the service account user with the assigned required roles, will not maintain the same privilege outside of the given project.

- ## Required GCP permissions
  - When you attach the Owner role to the service account that you create, you grant that service account all permissions, including those that are required to install OpenShift Container Platform. To deploy an OpenShift Container Platform cluster, the service account requires the following permissions. If you deploy your cluster into an existing VPC, the service account does not require certain networking permissions, which are noted in the following lists:
    - Required roles for the installation program:
      - **Compute Admin**
        - The Compute Admin gives full control of all compute resources. It is needed by the service account to manage virtual machine instances. OpenShift is a self managed/self healing platform that needs permissions to create cloud infrastructure to automatically scale and failover during normal operation.
      - **Security Admin**
        - This permission is needed to allow the service account to be able to create, modify, and delete firewall rules and SSL certificates, etc - within the gcp project
      - **Service Account Admin**
        - This role creates and manages service accounts
      - **Service Account User**
        - This roles runs operations as the service account
      - **Storage Admin**
        - This role Grants full control of storage objects and buckets and is needed to help provide persistent storage to the cluster.

- Required roles for creating network resources during installation:
  - **DNS Administrator**

- To install OpenShift Container Platform, the Google Cloud Platform (GCP) account you use must have a dedicated public hosted zone in the same project that you host the OpenShift Container Platform cluster. This zone must be authoritative for the domain. The DNS service provides cluster DNS resolution and name lookup for external connections to the cluster. Therefore the role is needed for the service account to provide read-write access to all Cloud DNS resources.

**Note:** Starting with OpenShift Container Platform 4.3, you do not need all of the permissions that are required for an installation program-provisioned infrastructure(IPI) install to deploy a cluster. This change mimics the division of permissions that you might have at your company: some individuals can create different resources in your clouds than others. For example, you might be able to create application-specific items, like instances, buckets, and load balancers, but not networking-related components such as VPCs, subnets, or Ingress rules.

The GCP credentials that you use when you create your cluster do not need the networking permissions that are required to make VPCs and core networking components within the VPC, such as subnets, routing tables, internet gateways, NAT, and VPN. You still need permission to make the application resources that the machines within the cluster require, such as load balancers, security groups, storage, and nodes.

Please see below roles for the service account the control plane and compute machines use:

| **Account** | **Roles** |
|---|---|
| **Control Plane** | roles/compute.instanceAdmin |
| | roles/compute.networkAdmin |
| | roles/compute.securityAdmin |
| | roles/storage.admin |
| | roles/iam.serviceAccountUser |
| **Compute** | roles/compute.viewer |
| | roles/storage.admin |

**Conclusion:** Based on whether installing in an existing VPC or a shared VPC, refer to the correct installation method and instructions at the links below.

Refer to the Supported installation methods for different platforms to choose the right method for your specific environment.

## References:

[1]https://docs.openshift.com/container-platform/4.6/installing/installing_gcp/installing-gcp-private.html#installation-about-custom-gcp-permissions_installing-gcp-private
[2]https://docs.openshift.com/container-platform/4.6/installing/installing_gcp/installing-gcp-account.html#installation-gcp-permissions_installing-gcp-account
[3]https://cloud.google.com/iam/docs/understanding-roles#compute-engine-roles

**Installing in an existing VPC:**
[4]https://docs.openshift.com/container-platform/4.6/installing/installing_gcp/installing-gcp-vpc.html

**Installing in a shared VPC:**
[5]https://docs.openshift.com/container-platform/4.6/installing/installing_gcp/installing-gcp-user-infra-vpc.html

**Installer-provisioned infrastructure (IPI):**

[6]https://docs.openshift.com/container-platform/4.6/installing/installing_gcp/installing-gcp-account.html#installation-gcp-permissions_installing-gcp-account

**User-provisioned infrastructure (UPI):**

[7]https://docs.openshift.com/container-platform/4.6/installing/installing_gcp/installing-gcp-user-infra-vpc.html#installation-gcp-permissions_installing-gcp-user-infra-vpc