  
  
  
**Step1**:For private clusters using VPC networks in the same project as the cluster, GKE ensures [Private Google Access](https://cloud.google.com/vpc/docs/private-google-access) is enabled on the subnet used by the private cluster when you create the cluster. A network admin, project owner, or project editor for a **Shared VPC host project must manually enable Private Google Access on subnets used by private clusters** if the private clusters are created in Shared VPC service projects.  
  
[Private Google Access](https://cloud.google.com/vpc/docs/private-google-access) is enabled by default in private clusters, except for Shared VPC clusters. You must enable Private Google Access manually for Shared VPC clusters.  
  
Private Google Access provides private nodes and their workloads access to Google Cloud APIs and services over Google's private network. For example, Private Google Access is required for private clusters to access container images from [Artifact Registry](https://cloud.google.com/artifact-registry/docs), and to send logs to [Cloud Logging](https://cloud.google.com/logging/docs).  
  
Step2: Unlike a public cluster, a private cluster has both a control plane private endpoint and a control plane public endpoint. You must specify a unique /28 IP address range for the control plane's private endpoint, and you can choose to disable the control plane's public endpoint.

Step3: Even though the nodes use internal IP addresses, external clients can connect to [Services](https://cloud.google.com/kubernetes-engine/docs/concepts/service) in your cluster. For example:

* An external client with a source IP address on the internet can connect to an external Service of type LoadBalancer if you omit spec.loadBalancerSourceRanges from the Service manifest.
* You can create a Service of type NodePort or ClusterIP and [expose the Service to external clients using an external Ingress](https://cloud.google.com/kubernetes-engine/docs/concepts/ingress-xlb).

Step4 : Private Google Access provides private nodes and their workloads access to Google Cloud APIs and services over Google's private network. For example, Private Google Access is required for private clusters to access container images from [Artifact Registry](https://cloud.google.com/artifact-registry/docs), and to send logs to [Cloud Logging](https://cloud.google.com/logging/docs).