Encrypt workload data in-use with Confidential Google Kubernetes Engine Nodes

STANDARD (/KUBERNETES-ENGINE/DOCS/CONCEPTS/TYPES-OF-CLUSTERS)

This page shows you how to enforce encryption of data in-use (https://wikipedia.org/wiki/Data_in_use) in your nodes and workloads using Confidential Google Kubernetes Engine Nodes.

Overview

Confidential GKE Nodes is built on top of Compute Engine Confidential VM (/compute/confidential-vm/docs/about-cvm), which encrypts the memory contents of VMs in-use. Encryption-in-use is one of the three states of end-to-end encryption.

When you enable Confidential GKE Nodes on a cluster or on a node pool, data in workloads running on the confidential nodes is encrypted-in-use. For visibility over your control plane, use Access Transparency (/access-transparency).

You can enable Confidential GKE Nodes when doing one of the following:

- Create a new cluster
- Create a new node pool
- Update an existing node pool

You cannot update an existing cluster to change the cluster-level Confidential GKE Nodes setting.

The following table shows you the GKE behavior that applies when you enable Confidential GKE Nodes at the cluster level or at the node pool level:

Confidential GKE Nodes setting	How to configure	Behavior
Cluster-level	Create a new cluster	All nodes in the cluster in any node pool use Confidential GKE Nodes. You **cannot** do the following:

		• Disable Confidential GKE Nodes for a new or existing node pool in the cluster • Disable Confidential GKE Nodes on the cluster • Enable Confidential GKE Nodes on existing clusters
Node pool level	• Create a new node pool • Update an existing node pool	You can only configure Confidential GKE Nodes for node pools when this feature disabled at the cluster-level.

Pricing

There is no additional cost to deploy Confidential GKE Nodes, other than the cost of Compute Engine Confidential VM (/compute/confidential-vm/pricing). However, Confidential GKE Nodes might generate slightly more log data on startup than standard nodes. For information on logs pricing, see Pricing for Google Cloud's operations suite (/stackdriver/pricing).

Availability

Confidential GKE Nodes is available in the following situations:

- Confidential GKE Nodes is only available in zones and regions with N2D instances (/compute/docs/machine-types#n2d_machine_types) or C2D instances (/compute/docs/compute-optimized-machines#c2d_machine_types) available.
- Confidential GKE Nodes can be used with Container-Optimized OS (/kubernetes-engine/docs/concepts/node-images#cos) and Container-Optimized OS with containerd (`cos_containerd`) (/kubernetes-engine/docs/concepts/using-containerd).

Before you begin

Before you start, make sure you have performed the following tasks:

- Enable the Google Kubernetes Engine API.

Enable Google Kubernetes Engine API (https://console.cloud.google.com/flows/enableapi?apiid

- If you want to use the Google Cloud CLI for this task, install (/sdk/docs/install) and then initialize (/sdk/docs/initializing) the gcloud CLI.

★ **Note:** For existing gcloud CLI installations, make sure to set the **`compute/region`** and **`compute/zone`** properties (/sdk/docs/properties#setting_properties). By setting default locations, you can avoid errors in gcloud CLI like the following: **`One of [--zone, --region] must be supplied: Please specify location`**.

Enable Confidential GKE Nodes on clusters

You can create a new cluster with Confidential GKE Nodes enabled by using the gcloud CLI or the Google Cloud console. If you enable Confidential GKE Nodes at the cluster level, all the nodes in the cluster are Confidential VM (/compute/confidential-vm/docs/about-cvm).

gcloudConsole (#console)
(#gcloud)

When creating a new cluster, specify the `--enable-confidential-nodes` option in the gcloud CLI:

```
gcloud container clusters create CLUSTER_NAME \
    --machine-type=MACHINE_TYPE \
    --enable-confidential-nodes
```

Replace the following:

- *CLUSTER_NAME*: the name of your new cluster.
- *MACHINE_TYPE*: the machine type for your cluster's default node pool, which must be the N2D machine type (/compute/docs/general-purpose-machines#n2d_machines) or the C2D machine type (/compute/docs/compute-optimized-machines#c2d_machine_types).

After creating a cluster with Confidential GKE Nodes, any node pools created in this cluster can only use confidential nodes. You cannot create regular node pools in clusters with

Confidential GKE Nodes enabled. You also cannot disable Confidential GKE Nodes on individual node pools when you enable Confidential GKE Nodes at the cluster level.

Enable Confidential GKE Nodes on node pools

You can enable Confidential GKE Nodes on specific node pools if Confidential GKE Nodes is disabled at the cluster level.

Create a new node pool

To create a new node pool with Confidential GKE Nodes enabled, run the following command:

```
gcloud container node-pools create NODE_POOL_NAME \
    --cluster=CLUSTER_NAME \
    --machine-type=MACHINE_TYPE \
    --enable-confidential-nodes
```

Replace the following:

- *NODE_POOL_NAME*: the name of your new node pool.
- *CLUSTER_NAME*: the name of your cluster.
- *MACHINE_TYPE*: the machine type for your node pool, which must be an N2D machine type (/compute/docs/machine-types#n2d_machine_types) or the C2D machine type (/compute/docs/compute-optimized-machines#c2d_machine_types).

Update an existing node pool

You can enable Confidential GKE Nodes on existing node pools that use the N2D machine type (/compute/docs/machine-types#n2d_machine_types) or the C2D machine type (/compute/docs/compute-optimized-machines#c2d_machine_types). Run the following command:

```
gcloud container node-pools update NODE_POOL_NAME \
    --cluster=CLUSTER_NAME \
    --enable-confidential-nodes
```

Replace the following:

- *NODE_POOL_NAME*: the name of your node pool.
- *CLUSTER_NAME*: the name of your cluster.

Verify that Confidential GKE Nodes are enabled

On clusters

You can verify that your cluster is using Confidential GKE Nodes with the gcloud CLI or the Google Cloud console.

gcloudConsole (#console)
(#gcloud)

Describe the cluster:

```
gcloud container clusters describe CLUSTER_NAME
```

If Confidential GKE Nodes is enabled, the output of the command includes the following lines:

```
confidentialNodes:
  enabled: true
```

On node pools

To verify that your node pool is using Confidential GKE Nodes, run the following command:

```
gcloud container node-pools describe NODE_POOL_NAME \
    --cluster=CLUSTER_NAME
```

If Confidential GKE Nodes is enabled, the output is similar to the following:

```
confidentialNodes:
  enabled: true
```

On nodes

To validate the confidentiality of specific nodes, you can:

1. Validate AMD SEV is enabled (/compute/confidential-vm/docs/creating-cvm-instance#verify-sev), or
2. Validate Confidential VM using Cloud Monitoring (/compute/confidential-vm/docs/monitoring).

Run applications on Confidential GKE Nodes

Google's approach to confidential computing is to enable an effortless lift and shift for existing applications. GKE workloads that you run today can run on Confidential GKE Nodes without code changes.

Optionally, if you want to declaratively express that your workloads must only run on clusters with Confidential GKE Nodes, you can use the **`cloud.google.com/gke-confidential-nodes`** node selector (https://kubernetes.io/docs/concepts/scheduling-eviction/assign-pod-node/#nodeselector). Here's an example Pod spec that uses this selector:

```
apiVersion: v1
kind: Pod
spec:
  containers:
  - name: my-confidential-app
    image: us-docker.pkg.dev/myproject/myrepo/my-confidential-app
    nodeSelector:
      cloud.google.com/gke-confidential-nodes:true
```

Set organization policy constraints

You can define an organization policy constraint to ensure that all VM resources created across your organization are Confidential VM instances. For GKE, you can customize the **Restrict Non-Confidential Computing** constraint to require that all new clusters are created with Confidential GKE Nodes enabled. Add the `container.googleapis.com` API Service name to the deny list when enforcing organization policy constraints (/compute/confidential-vm/docs/org-policy-constraints), for example:

```
gcloud resource-manager org-policies deny \
    constraints/compute.restrictNonConfidentialComputing compute.googleapis.c
    --project=PROJECT_ID
```

Replace ***PROJECT_ID*** with your project ID.

Limitations

Confidential GKE Nodes has the following limitations:

- Node auto-provisioning (/kubernetes-engine/docs/how-to/node-auto-provisioning) support on Confidential GKE Nodes with the C2D machine type (/compute/docs/compute-optimized-machines#c2d_machine_types) in GKE version 1.24 and later.
- Confidential GKE Nodes only supports PersistentVolumes (/kubernetes-engine/docs/concepts/persistent-volumes) backed by persistent disks (/compute/docs/disks#pdspecs) if your control plane runs GKE version 1.22 and later. For instructions, refer to Using the Compute Engine persistent disk CSI Driver (/kubernetes-engine/docs/how-to/persistent-volumes/gce-pd-csi-driver).
- Confidential GKE Nodes is not compatible with GPUs.
- Confidential GKE Nodes is not compatible with sole tenant nodes.
- Confidential GKE Nodes only supports using ephemeral storage on local SSDs (/kubernetes-engine/docs/how-to/persistent-volumes/local-ssd#creating_a_node_pool_using_ephemeral_storage_on_local_ssds) , but doesn't support using local SSDs in general.
- Only Container-Optimized OS nodes are supported. Ubuntu and Windows nodes are not supported.

Disable Confidential GKE Nodes

Disabling Confidential GKE Nodes only works for node pools that have enabled Confidential GKE Nodes. If the cluster is created with Confidential GKE Nodes, you cannot disable the feature. Run the following command to disable Confidential GKE Nodes on a node pool:

```
gcloud container node-pools update NODE_POOL_NAME \
    --cluster=CLUSTER_NAME \
    --no-enable-confidential-nodes
```

What's next

- Learn more about Confidential VM (/compute/confidential-vm/docs/about-cvm).
- Learn more about node images (/kubernetes-engine/docs/concepts/node-images).
- Learn more about Google Cloud encryption at rest (/security/encryption/default-encryption).
- Learn more about Google Cloud encryption in transit (/security/encryption-in-transit).
- Learn more about customer-managed encryption keys (CMEK) (/kubernetes-engine/docs/how-to/using-cmek).
- Learn more about application-layer secrets encryption (/kubernetes-engine/docs/how-to/encrypting-secrets).

Last updated 2022-09-28 UTC.