

# Secure DevOps – Assignment 1

## Task – 1: Setting Up Initial Infrastructure

### 1. Setting up Kubernetes Cluster on GKE.

The screenshot shows the Google Cloud Platform console for a project named 'ISEC6000'. The left sidebar displays the 'Kubernetes Engine' navigation menu with options like Clusters, Workloads, Services & Ingress, Applications, Secrets & ConfigMaps, Storage, Object Browser, Migrate to Containers, Backup for GKE, Security Posture, Config & Policy, and Config. The main content area is titled 'Clusters' and shows a list of clusters. The selected cluster is 'isec6000-secdevops-p1', which is in a 'Running' state. The 'DETAILS' tab is active, showing the following information:

Cluster basics		
Name	isec6000-secdevops-p1	🔒
Location type	Regional	🔒
Region	us-central1	🔒
Default node zones	us-central1-a us-central1-b us-central1-c us-central1-f	✎
Release channel	Regular channel	✎ UPGRADE AVAILABLE
Version	1.27.3-gke.100	
External endpoint	35.226.149.50	✎
	<a href="#">Show cluster certificate</a>	
Internal endpoint	10.128.0.2	🔒
	<a href="#">Show cluster certificate</a>	

The screenshot shows the 'Automation' tab for the same Kubernetes Engine cluster. It displays various settings that can be configured for the cluster's operation:

Automation		
Maintenance window	Any time	✎
Maintenance exclusions	None	
Notifications	Disabled	✎
Vertical Pod Autoscaling	Enabled	✎
Node auto-provisioning (Autopilot mode)	Enabled	✎
Auto-provisioning network tags		✎
Autoscaling profile	Optimize utilization	✎

Google Cloud

ISEC6000

Search (/) for resources, docs, products, and more

Search

Kubernetes Engine

Clusters

EDITDELETEDEPLOYCONNECTDUPLICATE

Clusters

Workloads

Services & Ingress

Applications

Secrets & ConfigMaps

Storage

Object Browser

Migrate to Containers

Backup for GKE

Security Posture

Config & Policy

Confia

Marketplace

Release Notes

<1

Networking

Private cluster	Disabled	🔒
Control plane global access	Disabled	✎
Network	<a href="#">default</a>	🔒
Subnet	<a href="#">default</a>	🔒
Stack type	IPv4	✎
Private control plane's endpoint subnet	<a href="#">default</a>	🔒
VPC-native traffic routing	Enabled	🔒
Pod IPv4 address range (default)	10.123.0.0/17	🔒
Cluster Pod IPv4 ranges (additional) ?	None	✎
IPv4 service range	34.118.224.0/20	🔒
Intranode visibility	Enabled	✎
HTTP Load Balancing	Enabled	✎
Subsetting for L4 Internal Load Balancers	Disabled	✎
Control plane authorized networks	Disabled	✎
Calico Kubernetes Network policy	Disabled	✎
Dataplane V2 ?	Enabled	🔒
DNS provider	Cloud DNS (cluster scope)	✎
NodeLocal DNSCache	Enabled	

Google Cloud

ISEC6000

Search (/) for resources, docs, products, and more

Search

Kubernetes Engine

Clusters

EDITDELETEDEPLOYCONNECTDUPLICATE

Clusters

Workloads

Services & Ingress

Applications

Secrets & ConfigMaps

Storage

Object Browser

Migrate to Containers

Backup for GKE

Security Posture

Config & Policy

Confia

Marketplace

Release Notes

<1

Metadata

Description	None	🔒
Labels	None	✎
Tags ?	None	✎

Features

Logging	System, Workloads <a href="#">View Logs</a>	✎
Cloud Monitoring	System <a href="#">View GKE Dashboard</a>	✎
Managed Service for Prometheus	Enabled	✎
Cloud TPU	Disabled	✎
Kubernetes alpha features	Disabled	🔒
Cost Allocation	Disabled	✎
GKE usage metering ?	Disabled	✎
Backup for GKE	Disabled ⓘ	✎
Config Connector	Disabled	✎
Compute Engine persistent disk CSI Driver	Enabled	✎
Image streaming	Enabled	✎
Filestore CSI driver	Enabled	✎
Anthos Service Mesh	Disabled	✎

Google Cloud ISEC6000

Search (/) for resources, docs, products, and more

Kubernetes Engine

Clusters EDIT DELETE DEPLOY CONNECT DUPLICATE

Clusters

- Workloads
- Services & Ingress
- Applications
- Secrets & ConfigMaps
- Storage
- Object Browser
- Migrate to Containers
- Backup for GKE
- Security Posture

Config & Policy

- Config
- Marketplace
- Release Notes

Security

Binary authorization	Disabled	
Shielded GKE nodes	Enabled	
Confidential GKE Nodes	Disabled	
Application-layer secrets encryption	Disabled	
Boot disk encryption	Google-managed	
Workload Identity	Enabled	
Workload identity namespace	woven-scene-396802.svc.id.goog	
Google Groups for RBAC	Disabled	
Legacy authorization	Disabled	
Basic authentication	Disabled	
Client certificate	Disabled	
Security posture	Enabled	
Workload vulnerability scanning	Enabled	

Metadata

Description	None	
Labels	None	
Tags	None	

## 2. Configuring kubectl to manage the kubernetes cluster.

Clusters

- Workloads
- Services & Ingress
- Applications
- Secrets & ConfigMaps
- Marketplace
- Release Notes

isec6000-secdevops-p1

DETAILS STORAGE OBSERVABILITY LOGS APP ERRORS

Cluster basics

Name	isec6000-secdevops-p1	
Location type	Regional	
Region	us-central1	
Default node zones	us-central1-a us-central1-b us-central1-c us-central1-f	

WELCOME TO CLOUD SHELL! Type "help" to get started.  
Your Cloud Platform project in this session is set to woven-scene-396802.  
Use "gcloud config set project [PROJECT\_ID]" to change to a different project.  
shovandeep\_tuladhar@cloudshell:~ (woven-scene-396802) \$ gcloud container clusters get-credentials isec6000-secdevops-p1 --region us-central1 --project woven-scene-396802  
Fetching cluster endpoint and auth data.  
kubeconfig entry generated for isec6000-secdevops-p1.  
shovandeep\_tuladhar@cloudshell:~ (woven-scene-396802) \$