Standard Operating Procedure (SOP)

Title

GCP Compute Engine – Virtual Machine Creation

Version

1.0

Purpose

This SOP defines standardized steps to create a **Google Cloud Compute Engine Virtual Machine** using both the **Google Cloud Console** and **gcloud CLI**, including security, networking, and operational best practices.

Scope

Applies to all teams provisioning Compute Engine VMs in GCP projects for **development, testing, staging, and production** workloads.

Responsibilities

- **Cloud / DevOps Engineer** – VM provisioning and configuration
- **Security Team** – Firewall rule and IAM review
- **Operations Team** – Monitoring, backup, and lifecycle management

Prerequisites

- Active GCP project
- Required IAM roles:
- Compute Admin
- Service Account User
- Billing enabled for the project
- gcloud CLI installed and authenticated (`gcloud auth login`)
- VPC network and subnet available
- SSH key configured (OS Login or project metadata)

---

1. VM Creation Using GCP Console

Step-by-Step Procedure

1. Log in to **Google Cloud Console**
2. Navigate to **Compute Engine → VM Instances**
3. Click **Create Instance**
4. Enter **Instance Name**
5. Select **Region** and **Zone**
6. Choose **Machine Configuration**
7. Series: E2 / N2 / C2
8. Machine Type: e2-medium, etc.
9. Select **Boot Disk Image**
10. Debian / Ubuntu / RHEL / Windows Server
11. Configure **Identity and API Access**
12. Service Account
13. Access scopes (least privilege)
14. Configure **Firewall Rules**
15. Allow SSH / RDP only if required
16. Configure **Networking, Disks, and Metadata**
17. Review configuration
18. Click **Create**

Output

- VM status: **Running**
- Internal/External IP assigned

---

2. VM Creation Using gcloud CLI

Command

```
gcloud compute instances create my-gcp-vm
  --zone=us-central1-a
  --machine-type=e2-medium
  --image-family=ubuntu-2204-lts
  --image-project=ubuntu-os-cloud
  --tags=ssh
```

Verify VM

```
gcloud compute instances list
```

---

3. Accessing the GCP VM

Linux VM

```
gcloud compute ssh my-gcp-vm --zone=us-central1-a
```

Windows VM

- Set Windows password from Console
- Connect using **Remote Desktop (mstsc)**

---

4. Security Best Practices

- Use **OS Login** instead of project-wide SSH keys
- Restrict firewall rules to specific source IPs
- Use **Service Accounts** with minimal permissions
- Enable **Shielded VM** features
- Enable **disk encryption** (default)

---

5. Networking Best Practices

- Avoid public IPs for backend workloads
- Use **Private Google Access**
- Use **Cloud Load Balancing** for public services
- Enable **VPC Flow Logs**

---

6. Cost Optimization Best Practices

- Choose appropriate machine families
- Stop or delete unused VMs
- Use **Committed Use Discounts**
- Use **preemptible/spot VMs** for non-critical workloads

---

7. Operational Best Practices

- Apply consistent **labels**
- name
- environment
- owner
- cost-center

- Enable **Cloud Monitoring and Logging**
- Schedule **snapshots** for persistent disks
- Use **OS Patch Management**

---

8. Validation Checklist

- VM is running
- SSH/RDP access verified
- Firewall rules validated
- Monitoring enabled
- Labels applied

---

9. Approval

Role	Name	Date
Cloud Architect		
Security Lead		