**📦 Google Artifact Registry – Overview**

**Google Artifact Registry** is a fully-managed service by Google Cloud for storing and managing **build artifacts** such as Docker images, language packages (like npm, Maven, Python, Go), and Helm charts.

**🔧 Key Features**

| **Feature** | **Description** |
| --- | --- |
| **Multi-format support** | Supports Docker, Maven, npm, Python, Go modules, Helm |
| **Regional** | Data is stored in specific GCP regions to reduce latency |
| **IAM-controlled access** | Fine-grained access control using IAM roles |
| **VPC-SC compatible** | Supports security perimeters |
| **GCR Integration** | You can migrate from [gcr.io](http://gcr.io) to Artifact Registry |

**✅ Common Use Cases**

* Store **Docker images** used in GKE, Cloud Run, or Compute Engine
* Host **language-specific packages** for CI/CD pipelines
* Enable **secure sharing** of internal packages across teams
* Migrate from **Container Registry (GCR)** to Artifact Registry

**📚 Artifact Formats Supported**

| **Format** | **Repository Type** | **Example** |
| --- | --- | --- |
| Docker | docker | [us-docker.pkg.dev/my-project/my-repo/my-image](http://us-docker.pkg.dev/my-project/my-repo/my-image) |
| Maven | maven | Java packages |
| npm | npm | Node.js packages |
| Python | python | PyPI |
| Go | go | Go modules |
| Helm | helm | Kubernetes Helm charts |

**🏗️ How to Use Artifact Registry for Docker**

**1. Enable Artifact Registry API**

gcloud services enable [artifactregistry.googleapis.com](http://artifactregistry.googleapis.com)

**2. Create a Docker Repository**

gcloud artifacts repositories create my-docker-repo \

--repository-format=docker \

--location=us-central1 \

--description="Docker repository"

**3. Configure Docker to Use Artifact Registry**

gcloud auth configure-docker [us-central1-docker.pkg.dev](http://us-central1-docker.pkg.dev)

**4. Push an Image**

docker tag my-image [us-central1-docker.pkg.dev/my-project/my-docker-repo/my-image](http://us-central1-docker.pkg.dev/my-project/my-docker-repo/my-image)

docker push [us-central1-docker.pkg.dev/my-project/my-docker-repo/my-image](http://us-central1-docker.pkg.dev/my-project/my-docker-repo/my-image)

**🔐 IAM Roles for Access**

| **Role** | **Permissions** |
| --- | --- |
| roles/artifactregistry.reader | Read-only access |
| roles/artifactregistry.writer | Read and write access |
| roles/artifactregistry.admin | Full control |

You can also grant these roles to users, service accounts, or groups at project/repo level.

**🔄 GCR Migration**

All traffic to [gcr.io](http://gcr.io) can be automatically redirected to Artifact Registry by enabling **migration mode**. You should:

* Move images from [gcr.io](http://gcr.io) to Artifact Registry using gcloud or scripts.
* Update deployment manifests with new image paths.

**📈 Monitoring & Security**

* Integrated with **Cloud Audit Logs**
* Can be monitored with **Cloud Monitoring**
* Supports **customer-managed encryption keys (CMEK)**