

**Set Up the Kubernetes Cluster**

1. **Choose a Kubernetes Provider**:
   * You can use a managed Kubernetes service like Amazon EKS, Google Kubernetes Engine (GKE), Azure Kubernetes Service (AKS)
   * Ensure nodes (worker and master) are distributed across multiple availability zones for high availability and fault tolerance

**Secure the Network**

1. **Create Separate Network Segments**:
   * Create separate network segments or virtual networks for your Kubernetes cluster and internal systems. Use VPC (Virtual Private Cloud) or similar network constructs provided by your cloud provider.
2. **Set Up Network Policies**:
   * Use Kubernetes Network Policies to restrict traffic between pods. Only allow necessary communication between the API services and internal systems

**VPC Peering or VPN**:

* Set up VPC peering or a VPN to securely connect your Kubernetes cluster network with the internal-assets virtual network. Ensure that this connection is encrypted and authenticated.

**Secure the Kubernetes Cluster**

1. **RBAC**:
   * Configure Role-Based Access Control (RBAC) to ensure that only authorized users and services can access the Kubernetes API and resources.

**Use TLS/SSL**:

* Ensure all communications within the cluster, as well as between the public API and clients, are encrypted using TLS/SSL. Use cert-manager to automatically provision and manage TLS certificates.

**Pod Security Policies**:

* Implement Pod Security Policies or the newer Pod Security Standards to control the security contexts under which pods run.

**Deploy Web Services**

1. **Create Kubernetes Deployments**:
   * Define and apply Kubernetes Deployment manifests for your web services.

**Create Services and Ingress**:

* Define Kubernetes Services and Ingress resources to expose your web services.
* **Install Monitoring Tools**:
  + Deploy monitoring tools like Prometheus, Grafana, and other relevant tools to monitor the health and performance of your services.
* **Centralized Logging**:
  + Use centralized logging solutions like Elasticsearch, Fluentd, and Kibana (EFK stack) or Loki to aggregate and analyze logs from your services.
  + Keep your Kubernetes cluster and related software up to date with the latest security patches and updates.