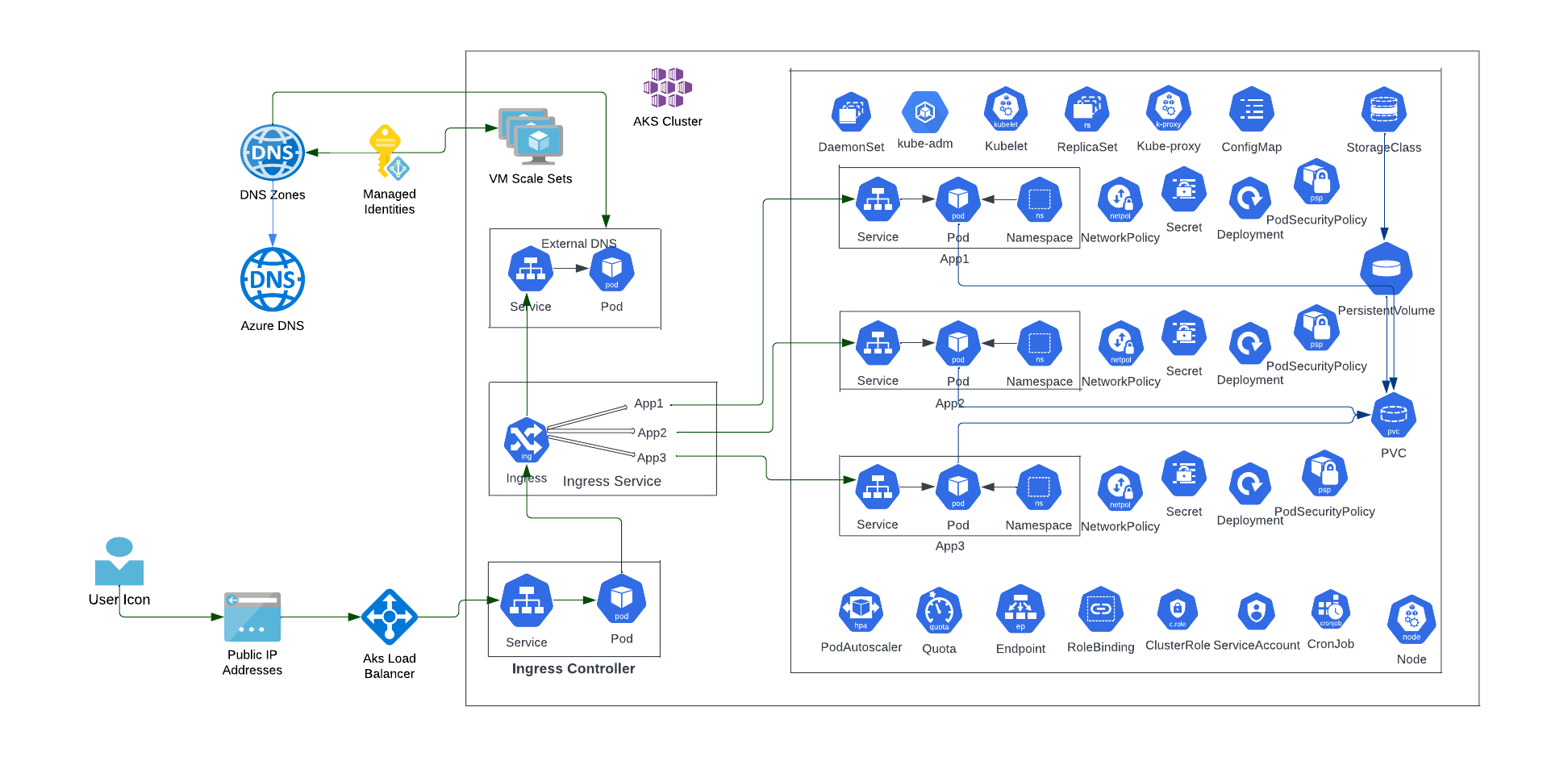
**AKS Architecture:**



**AKS Architecture Consideration:**

1. **Azure Well Architected Framework**

1. **Capacity Analysis:**

* Regions Availability
* Restricted VM size
* Node Operating system
* Kubernetes version
* Network
* Resource reservation
* Subscription and Resource Group Limits

1. **Compute Requirement:**

* Compute Size
* Region
* Reserved compute

1. **Storage Analysis:**
   * Type of storage
   * Long term storage or short term
   * Need to archive
   * Private or public traffic
   * Security in storage Account
   * Files or Disk

4. **Networking Components:**

* Vnet Address space
* Pod CIDR
* Service CIDR
* DNS IP
* Docker Bridge CIDR
* Core DNS vs Kube DNS and Name Server
* CIDR cannot Overlap each other
* Enough IP's in Subnets for POD's

1. **Kubenet vs Azure CNI**

* Pros and Cons
* Route table, IP address, POD limitations, Network policies

1. **Services - Cluster IP and Ingress:**

* Nginx Ingress or Azure Ingress

1. **Load Balancer Consideration**

* Basic vs Standard
* Regional or Global
* DNS or HTTP
* Failover, SSL and WAF
* SLA and Availability

1. **App Gateway Load Balancer:**

* Kubenet - Route table Reference for traffic
* Azure CNI - Route directly to Pods through App config files.

1. **External DNS or Azure DNS**

* Name server and Records
* Core DNS and Cluster DNS
* External DNS or Azure DNS

1. **Network Security Groups**

* Whitelisting Ip
* Inbound traffic

1. **AKS Network Egress Traffic:**

* Basic External Load Balancer with Dynamic outbound ip
* Basic External Load Balancer with Static outbound ip
* Standard External Load Balancer - Outbound rules & NAT
* Standard External Load Balancer customization (To avoid SNAT port)
* Internal network egress (CNI -> Outbound ip -> POD ip) & (kubenet -> Outbound IP -> Cluster Subnet)

1. **AKS Network Ingress Traffic:**

* Ingress Traffic from the Internet
* Nginx-ingress / cert-manager
* Http Application Routing
* Ingress traffic from Internal network

**5. Site Recovery Strategy / High Availability**

Multiple Regions Deployment

RPO/RTO/SLA

Resiliency

Zone Redundant AZ

**6. Azure AKS Security Baseline**

* Azure AD integration
* Master Security
* Node Security
* Cluster Upgrades
* Network security
* Pod security
* Container Image scanning
* Central security log management
* Establish secure configurations for all Azure Resources
* Scan for vulnerabilities
* Network policies
* TLS and Certificates Enablement

**7. Integrations**

**8. Monitoring**

**9. Type of Deployment**

**10. Migration Strategy**