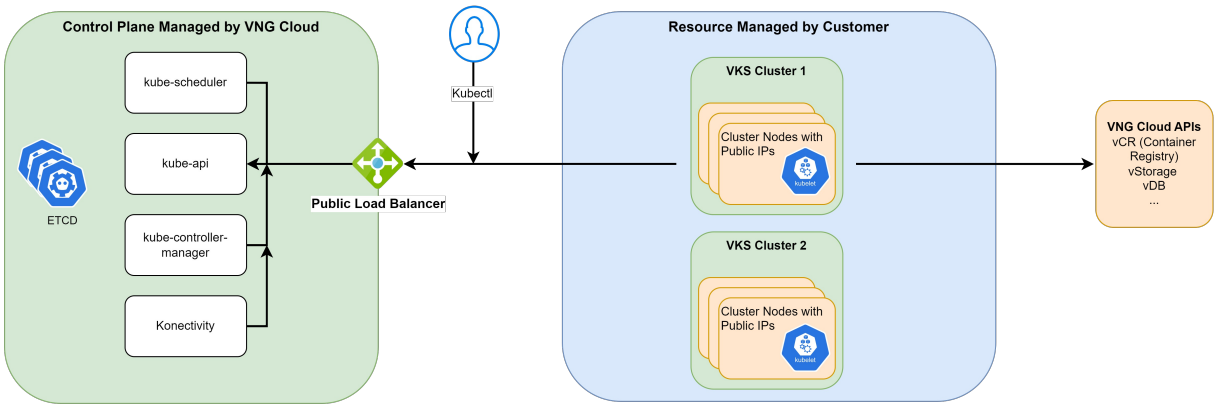
Mô hình hoạt động

Bên dưới là các concepts hiện tại VKS đang cung cấp cho bạn:

1. Public Cluster



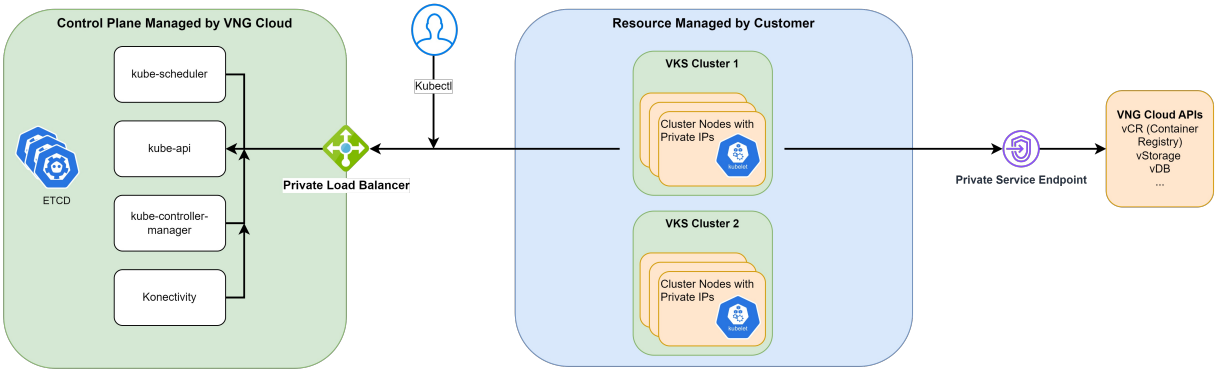
Khi bạn khởi tạo một **Public Cluster với Public Node Group**, hệ thống VKS sẽ:

- Tạo VM có Floating IP (tức có IP Public). Lúc này các VM (Node) này có thể join trực tiếp vào cụm K8S thông qua Public IP này. Bằng cách sử dụng Public Cluster và Public Node Group, bạn có thể dễ dàng tạo các cụm Kubernetes và thực hiện expose service mà không cần sử dụng Load Balancer. Việc này sẽ góp phần tiết kiệm chi phí cho cụm của bạn.

Khi bạn khởi tạo một **Public Cluster với Private Node Group**, hệ thống VKS sẽ:

- Tạo VM không có Floating IP (tức không có IP Public). Lúc này các VM (Node) này không thể join trực tiếp vào cụm K8S. Để các VM này có thể join vào cụm K8S, bạn cần phải sử dụng một NAT Gateway (**NATGW**). **NATGW** hoạt động như một trạm chuyển tiếp, cho phép các VM kết nối với cụm K8S mà không cần IP Public. Với VNG Cloud, chúng tôi khuyến cáo bạn sử dụng Pfsense hoặc Palo Alto như một NATGW cho Cluster của bạn. Pfsense sẽ giúp bạn quản lý lưu lượng mạng đến và đi (inbound và outbound traffic) một cách hiệu quả, đảm bảo an ninh mạng và quản lý truy cập. Bên cạnh đó, việc sử dụng Private Node Group sẽ giúp bạn kiểm soát các ứng dụng trong cụm được bảo mật hơn, cụ thể bạn có thể thực hiện giới hạn quyền truy cập control plane thông qua tính năng Whitelist IP.

2. Private Cluster



Khi bạn khởi tạo một **Private Cluster với Public/ Private Node Group**, hệ thống VKS sẽ:

- Để nâng cao bảo mật cho cluster của bạn, chúng tôi đã cho ra mắt mô hình private cluster.

Tính năng Private Cluster giúp cho cụm K8S của bạn được bảo mật nhất có thể, mọi kết nối hoàn toàn là private từ kết nối giữa nodes tới control plane, kết nối từ client tới control plane, hay kết nối từ nodes tới các sản phẩm dịch vụ khác trong VNG Cloud như: vStorage, vCR, vMonitor, VNGCloud APIs,...Private Cluster là lựa chọn lý tưởng cho **các dịch vụ yêu cầu kiểm soát truy cập chặt chẽ, đảm bảo tuân thủ các quy định về bảo mật và quyền riêng tư dữ liệu**.

---

3. So sánh giữa việc sử dụng Public Cluster và Private Cluster

Dưới đây là bảng so sánh giữa việc tạo và sử dụng Public Cluster và Private Cluster trên hệ thống VKS:

Tiêu chí	Public Cluster	Private Cluster
Kết nối	Sử dụng địa chỉ Public IP để giao tiếp giữa nodes và control plane, giữa client và control plane, giữa nodes và các dịch vụ khác trong VNG Cloud.	Sử dụng địa chỉ Private IP để giao tiếp giữa nodes và control plane, giữa client và control plane, giữa nodes và các dịch vụ khác trong VNG Cloud.
Bảo mật	Bảo mật trung bình do các kết nối sử dụng Public IP.	Bảo mật cao hơn với tất cả kết nối đều private và giới hạn truy cập.
Quản lý truy cập	Khó kiểm soát hơn, có thể quản lý truy cập thông qua tính năng Whitelist	Kiểm soát truy cập chặt chẽ, mọi kết nối đều nằm trong mạng private của VNG Cloud, từ đó giảm thiểu nguy cơ từ các cuộc tấn công mạng từ bên ngoài.
Khả năng mở rộng (AutoScaling)	Dễ dàng mở rộng thông qua tính năng **Auto Scaling**.	Dễ dàng mở rộng thông qua tính năng **Auto Scaling**.
Khả năng tự hồi phục (AutoHealing)	Tự động phát hiện lỗi và khởi động lại node (**Auto Healing**)	Tự động phát hiện lỗi và khởi động lại node (**Auto Healing**)
Khả năng truy cập từ bên ngoài	Dễ dàng truy cập từ bất kỳ đâu với internet.	Truy cập từ bên ngoài phải qua các giải pháp bảo mật khác.
Cấu hình và triển khai	Đơn giản hơn do không yêu cầu thiết lập mạng nội bộ.	Phức tạp hơn, yêu cầu cấu hình mạng private và bảo mật.
Chi phí	Thường thấp hơn do không cần thiết lập cơ sở hạ tầng bảo mật phức tạp.	Chi phí cao hơn do yêu cầu thêm các thành phần bảo mật và quản lý. **Cụ thể, khi sử dụng private cluster, bạn cần chi trả chi phí cho 4 private service endpoint được tạo tự động để kết nối tới các dịch vụ trên VNG Cloud.**
Tính linh hoạt	Cao, dễ dàng thay đổi và truy cập các dịch vụ.	Linh hoạt hơn trong các ứng dụng yêu cầu bảo mật, nhưng ít linh hoạt hơn cho các ứng dụng yêu cầu truy cập từ bên ngoài.

Do đó:

- **Public Cluster**: Phù hợp cho các ứng dụng không yêu cầu bảo mật cao và cần sự linh hoạt, truy cập từ nhiều địa điểm. Dễ dàng triển khai và quản lý nhưng có rủi ro bảo mật cao hơn.
- **Private Cluster**: Phù hợp cho các ứng dụng yêu cầu bảo mật cao, tuân thủ nghiêm ngặt các quy định về bảo mật và quyền riêng tư. Mang lại kết nối ổn định và bảo mật, nhưng yêu cầu cấu hình và quản lý phức tạp hơn, cũng như chi phí cao hơn.