3. Mô hình hoạt động của VKS

- VNGCloud Kubernetes Service (VKS) hỗ trợ 2 loại cluster chính là **Public Cluster** và **Private Cluster**. Đối với node group, VKS hỗ trợ 2 loại node group chính là **Public Node Group** và **Private Node Group**. Từ đó, khách hàng có thể kết hợp giữa các loại cluster và node group để tạo ra các mô hình hoạt động phù hợp với yêu cầu của ứng dụng, cụ thể:
  - Public Cluster với Public Node Group: Các node trong nodegroup có địa chỉ IP Public riêng, kết đến nối ControlPlane thông qua IP Public của Kubernetes API Server. Điều này dẫn rủi ro bảo mật cao hơn. Tuy nhiên bạn hoàn toàn có thể hạn chế truy cập đến ControlPlane thông qua tính năng Whitelist IP. Một điều lưu ý là bạn cần đảm bảo không hạn chế truy cập từ các IP của các node trong nodegroup.
  - Public Cluster với Private Node Group: Các node trong nodegroup không có địa chỉ IP Public riêng, không thể kết nối trực tiếp đến ControlPlane. Để các node trong nodegroup có thể kết nối đến ControlPlane, bạn cần sử dụng một NAT Gateway (NATGW). NATGW hoạt động như một trạm chuyển tiếp, cho phép các node kết nối với ControlPlane mà không cần IP Public. VNGCloud khuyến nghị sử dụng Pfsense hoặc Palo Alto như một NATGW cho Cluster của bạn.
  - Private Cluster với Public Node Group: Các node trong nodegroup có địa chỉ IP Public riêng, kết đến nối ControlPlane thông qua IP Private của Kubernetes API Server. Điều này giúp giảm rủi ro bảo mật.
  - Private Cluster với Private Node Group: Các node trong nodegroup không có địa chỉ IP Public riêng, mọi kết nối đến Kubernetes API server đều thông qua IP Private. Điều này giúp tăng cường bảo mật cho cụm Kubernetes của bạn.

3.1. So sánh 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:
  - Kết nối:
    - Public cluster: 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.
    - Private cluster: 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:
    - Public cluster: Bảo mật trung bình do các kết nối sử dụng Public IP.
    - Private cluster: Bảo mật cao hơn với tất cả kết nối đều private và giới hạn truy cập.
  - Quản lý truy cập:

        - Public cluster: Khó kiểm soát hơn, có thể quản lý truy cập thông qua tính năng Whitelist.
        - Private cluster: 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):
        - Public cluster: Dễ dàng mở rộng thông qua tính năng Auto Scaling.
        - Private cluster: Dễ dàng mở rộng thông qua tính năng Auto Scaling.
    - Khả năng tự hồi phục (AutoHealing):
        - Public cluster: Tự động phát hiện lỗi và khởi động lại node (Auto Healing)
        - Private cluster: Tự động phát hiện lỗi và khởi động lại node (Auto Healing)
    - Khả năng truy cập từ bên ngoài:
        - Public cluster: Dễ dàng truy cập từ bất kỳ đâu với
        - Private cluster: Truy cập từ bên ngoài phải qua các giải pháp bảo mật khác.
    - Cấu hình và triển khai:
        - Public cluster: Đơn giản hơn do không yêu cầu thiết lập mạng nội bộ.
        - Private cluster: Phức tạp hơn, yêu cầu cấu hình mạng private và bảo mật.
    - Chi phí:
        - Public cluster: Thường thấp hơn do không cần thiết lập cơ sở hạ tầng bảo mật phức tạp.
        - Private cluster: 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 VNGCloud.
    - Tính linh hoạt:
        - Public cluster: Cao, dễ dàng thay đổi và truy cập các dịch vụ.
        - Private cluster: 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.
- Kết luận:
    - 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.