|  |
| --- |
| BAN CƠ YẾU CHÍNH PHỦ  **HỌC VIỆN KỸ THUẬT MẬT MÃ**  ¯¯¯¯¯¯¯¯¯¯¯¯¯¯¯¯ |
| ĐỀ CƯƠNG ĐỒ ÁN TỐT NGHIỆP  **[Nghiên cứu giải pháp đảm bảo an toàn cho microservices trên k8s cluster với Consul Service Mesh]** |
| Ngành: An toàn thông tin  Mã số: 7.48.02.02  *Sinh viên thực hiện*:  **Nguyễn Anh Tuấn**  Lớp: AT16BT  *Người hướng dẫn*:  **TS. Nguyễn Mạnh Thắng**  Khoa An toàn thông tin – Học viện Kỹ thuật mật mã |
| **Hà Nội, 2023** |

# Mở đầu

## Tính cấp thiết của đề tài

Trong sự phát triển của công nghệ vào những thời điểm gần đây, kiến trúc các ứng dụng dịch vụ của các doanh nghiệp là một trong những phần mà khiến cho các doanh nghiệp đáng phải quan tâm. Ngày trước, với khuôn mẫu cổ điển là kiến trúc một khối, các ứng dụng dịch vụ được triển khai rất dễ dàng. Tuy nhiên, khi cần phải giải quyết tính sẵn sàng của các ứng dụng dịch vụ, các tài nguyên bao gồm phần cứng cũng như con người để phát triển và vận hành chúng cực kì khó khăn. Vì vậy, để giải quyết vấn đề trên, sự ra đời của kiến trúc microservice đã giải quyết được một phần nào đấy trên vấn đề trên. Microservices linh hoạt hơn trong việc xử lý các API với nhau, chúng có thể được tích hợp với các ứng dụng khác thông qua REST hoặc các message queue như Kafka,... Tuy nhiên, để đảm bảo về tính bảo mật và an toàn trong một hệ thống microservices, việc xác thực giữa các microservice là một vấn đề khá nhức nhối cho đội phát triển ứng dụng.

Để giúp cho đội phát triển có thể phát triển ứng dụng một cách dễ dàng nhất, việc nghiên cứu bảo mật giữa các microservice sẽ được chuyển lại cho đội vận hành. Nghiên cứu trong việc đảm bảo an toàn giữa các ứng dụng thành công nhất là Service Mesh, một trong những giải pháp được áp dụng vào nhiều doanh nghiệp lớn hiện nay không chỉ trên thế giới mà ở Việt Nam cũng được sử dụng rất nhiều.

Để nghiên cứu thêm về Service Mesh, em đã chọn đề tài này nhằm tìm hiểu về Service Mesh, phương thức hoạt động của Service Mesh ra sao, làm thế nào Service Mesh giúp đảm bảm cho tính bảo mật giữa các microservices với nhau trong hệ thống thông tin hiện nay.

## Mục tiêu thực hiện đồ án

Mục tiêu của đồ án này là nghiên cứu và thực hiện giải pháp bảo mật giữa các microservice với nhau thông qua Service Mesh. Mục tiêu chính của đề tài:

* Tìm hiểu về công nghệ Container, kiến trúc microservice ở trong thời điểm hiện tại.
* Tổng quan về Kubernetes, microservices được sử dụng trên hệ thống kuberentes.
* Tìm hiểu về các thức hoạt động, triển khai và vận hành của Service Mesh trong Kubernetes.
* Đảm bảo tính bảo mật giữa các microservice được triển khai và vận hành trên hệ thống Kubernetes thông qua Service Mesh.

# Dự kiến các Chương, mục

1. Giới thiệu về công nghệ Container và kiến trúc Microservices
   1. Giới thiệu về công nghệ Container
      1. Tìm hiểu về công nghệ Container
      2. Container và máy ảo
      3. Đặc điểm của Container
      4. Ứng dụng của container trong thực tế
      5. Containerization
      6. Thách thức trong việc sử dụng Container
   2. Giới thiệu về kiến trúc Microservices
      1. Khái niệm về kiến trúc Microservices
      2. Ưu điểm của kiến trúc Microservices
      3. Các nhược điểm của kiến trúc Microservices
      4. Những yêu cầu bắt buộc khi phát triển ứng dụng theo kiến trúc Microservices
   3. Giới thiệu về Kubernetes
      1. Kiến trúc của Kubernetes
      2. Tổng quan về Pod
      3. Vòng đời của Pod
      4. Quản lý Pod bằng workload trên Kubernetes
   4. Một số vấn đề bảo mật Microservices trên Kubernetes
      1. Khả năng bị tấn công của các ứng dụng Microservices
      2. Kiểm tra bảo mật làm giảm các hiệu suất
      3. Sự phức tạp khi triển khai xác thực giữa các Microservices
      4. Khó khan của các Developer đối với Microservices

Kết luận Chương 1

1. Giới thiệu về HashiCorp Consul
   1. Tổng quan về Service Mesh
      1. Phương thức hoạt động của Service Mesh
      2. Các tính năng của Service Mesh
      3. Tổng quan về Envoy Proxy
   2. Tổng quan về Consul
      1. Kiến trúc của Consul
      2. Consul so với các Service Mesh khác
      3. Các tính năng khác của Consul
   3. Bảo mật các Microservice bằng Consul
      1. Zero trust network trong Consul
      2. Mã hoá trong Consul
      3. Xác thực trong Consul
      4. Uỷ quyền trong Consul

Kết luận Chương 2

1. Triển khai Consul trên Kubernetes
   1. Mô hình thực nghiệm
   2. Các bước triển khai Consul trên Kubernetes
   3. Kịch bản thực nghiệm

Kết luận Chương 3

# Tài liệu tham khảo

[] Consul: Up and Running, Luke Kysow, 2022

[2] Microservices Security In Action, Prabath Siriwardena, 2020

[] Kubernetes in Action, Marko Luksa, 2018

[] Documentation. Online: <https://developer.hashicorp.com/consul/docs>

[5] Documenation. Online: <https://kubernetes.io/docs/home/>

|  |  |  |
| --- | --- | --- |
|  |  | *Hà Nội, ngày 19 tháng 06 năm 2023* |
| **XÁC NHẬN CỦA NGƯỜI HƯỚNG DẪN CHÍNH**  *(Ký, ghi rõ họ tên)* |  | **SINH VIÊN THỰC HIỆN**  *(Ký, ghi rõ họ tên)* |
| **Nguyễn Mạnh Thắng** |  | **Nguyễn Anh Tuấn** |