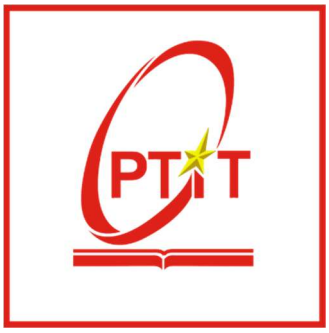
HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH VIỄN THÔNG



VŨ TUẤN NHẬT

Đề cương

ĐỀ ÁN TỐT NGHIỆP THẠC SĨ KỸ THUẬT

(Theo định hướng ứng dụng)

HÀ NỘI – 2024

HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH VIỄN THÔNG

VŨ TUẤN NHẬT

XÂY DỰNG GIẢI PHÁP TĂNG CƯỜNG BẢO MẬT CHO NỀN TẢNG KUBERNETES TẠI VNPT HÀ NỘI

Chuyên ngành: Hệ thống thông tin

Mã số: 8.48.01.04

Đề cương đề án tốt nghiệp thạc sĩ kỹ thuật

(Theo định hướng ứng dụng)

Người hướng dẫn khoa học: PGS.TS HOÀNG XUÂN DẬU

HÀ NỘI – 2024

I. Mở đầu

1. Lý do chọn đề tài

Trong bối cảnh công nghệ thông tin phát triển nhanh chóng, Kubernetes (K8S) đã trở thành nền tảng quản lý container phổ biến nhất, được nhiều doanh nghiệp, trong đó có VNPT Hà Nội, áp dụng để tối ưu hóa việc triển khai và quản lý ứng dụng. Tuy nhiên, sự phổ biến này cũng đi kèm với những thách thức về bảo mật, khi K8S trở thành mục tiêu hấp dẫn cho các cuộc tấn công mạng. Hiện trạng bảo mật của K8S tại VNPT Hà Nội, được triển khai trên hạ tầng đơn vị, đang đối mặt với nhiều vấn đề như cấu hình không an toàn, quản lý quyền truy cập chưa chặt chẽ, và thiếu các biện pháp giám sát hiệu quả. Những lỗ hổng này không chỉ đe dọa đến hoạt động của hệ thống mà còn có thể gây ra thiệt hại lớn về dữ liệu và uy tín của doanh nghiệp.

Việc triển khai K8S trên hạ tầng đơn vị mang lại nhiều lợi ích như kiểm soát hoàn toàn về mặt phần cứng, mạng nội bộ và dữ liệu, nhưng đồng thời cũng tạo ra những thách thức riêng về bảo mật. Hạ tầng đơn vị thường thiếu các biện pháp bảo mật tiên tiến mà các dịch vụ đám mây cung cấp sẵn, đòi hỏi VNPT Hà Nội phải tự xây dựng và duy trì các giải pháp bảo mật hiệu quả để bảo vệ hệ thống của mình.

Việc tăng cường bảo mật cho nền tảng Kubernetes tại VNPT Hà Nội là vô cùng cần thiết để đảm bảo tính toàn vẹn, bảo mật và khả năng phục hồi của các ứng dụng triển khai trên nền tảng này. Các yêu cầu cần được tăng cường bao gồm:

- Cấu hình bảo mật: đảm bảo rằng tất cả các thành phần của K8S được cấu hình theo các nguyên tắc bảo mật tốt nhất, giảm thiểu tối đa các lỗ hổng có thể bị khai thác.
- Quản lý quyền truy cập: thiết lập các cơ chế kiểm soát truy cập mạnh mẽ để đảm bảo rằng chỉ những người dùng và dịch vụ được ủy quyền mới có thể truy cập và thao tác với các tài nguyên quan trọng.
- Giám sát và phát hiện xâm nhập: triển khai các hệ thống giám sát liên tục và các công cụ phát hiện xâm nhập để kịp thời phát hiện và phản ứng với các hoạt động bất thường hoặc có dấu hiệu tấn công.
- Bảo mật mạng nội bộ: tăng cường bảo mật cho các giao tiếp mạng giữa các thành phần trong K8S, bao gồm việc sử dụng mã hóa dữ liệu và thiết lập các chính sách mạng nghiêm ngặt trên hạ tầng đơn vị.

- Quản lý bản vá và cập nhật: đảm bảo rằng tất cả các thành phần của K8S và các ứng dụng liên quan luôn được cập nhật các bản vá bảo mật mới nhất để phòng chống các mối đe dọa hiện tại và tương lai.

Việc nghiên cứu và xây dựng các giải pháp tăng cường bảo mật cho K8S tại VNPT Hà Nội không chỉ giúp bảo vệ hệ thống hiện tại mà còn tạo nền tảng vững chắc cho việc mở rộng và phát triển trong tương lai. Đồng thời, nó cũng góp phần nâng cao nhận thức về bảo mật trong toàn bộ tổ chức, từ đó tạo ra một môi trường làm việc an toàn và tin cậy hơn..

2. Tổng quan về vấn đề nghiên cứu

Kubernetes (K8S) đã chứng minh được sức mạnh và tính linh hoạt trong việc quản lý và triển khai các ứng dụng container hóa. Tuy nhiên, sự phức tạp và quy mô của K8S cũng mang lại nhiều thách thức về bảo mật, đặc biệt khi triển khai trên hạ tầng đơn vị. Để đảm bảo và tăng cường bảo mật cho K8S, có nhiều giải pháp đã được nghiên cứu và triển khai, từ các phương pháp cơ bản đến những công nghệ tiên tiến. Dưới đây là một số giải pháp chính được khảo sát:

2.1. Cấu hình bảo mật Kubernetes

Một trong những yếu tố quan trọng nhất để bảo mật K8S là cấu hình chính xác và an toàn. Việc cấu hình sai hoặc không đầy đủ có thể dẫn đến các lỗ hổng bảo mật nghiêm trọng. Các khuyến nghị bao gồm:

- Bật và cấu hình rbac (role-based access control): rbac giúp kiểm soát quyền truy cập vào các tài nguyên K8S dựa trên vai trò của người dùng hoặc dịch vụ.
- Sử dụng mạng nội bộ riêng biệt: tách biệt các thành phần mạng nội bộ để hạn chế phạm vi ảnh hưởng của các cuộc tấn công.
- Mã hóa dữ liệu: sử dụng tls để mã hóa dữ liệu truyền tải giữa các thành phần của K8S và sử dụng các giải pháp mã hóa dữ liệu lưu trữ trên hạ tầng đơn vị.

2.2. Quản lý thông tin quan trọng và cấu hình

Thông tin quan trọng như mật khẩu, khóa api và chứng chỉ là yếu tố quan trọng trong bảo mật K8S. Các giải pháp quản lý thông tin quan trọng bao gồm:

- Sử dụng Kubernetes secrets: lưu trữ và quản lý thông tin quan trọng một cách an toàn trong K8S.

- Tích hợp với các hệ thống quản lý thông tin quan trọng bên ngoài: sử dụng các giải pháp như hashicorp vault để quản lý thông tin quan trọng một cách hiệu quả và bảo mật hơn trên hạ tầng đơn vị.

2.3. Giám sát và phát hiện xâm nhập

Việc giám sát liên tục và phát hiện các hoạt động bất thường là yếu tố then chốt để bảo vệ hệ thống K8S. Các giải pháp bao gồm:

- Sử dụng các công cụ giám sát như prometheus và grafana: theo dõi các chỉ số hiệu suất và trạng thái của K8S.
- Triển khai hệ thống phát hiện xâm nhập (ids): sử dụng các công cụ như falco để phát hiện các hành vi bất thường trong môi trường K8S.

2.4. Bảo mật mạng nội bộ

Bảo mật mạng trong K8S bao gồm việc kiểm soát lưu lượng mạng giữa các pod và các dịch vụ. Các giải pháp bao gồm:

- Sử dụng network policies: định nghĩa các chính sách mạng để kiểm soát lưu lượng giữa các pod.
- Triển khai service mesh: sử dụng các giải pháp như istio để quản lý giao tiếp giữa các dịch vụ, bao gồm mã hóa và kiểm soát truy cập.

2.5. Quản lý bản vá và cập nhật

Đảm bảo rằng tất cả các thành phần của K8S và các ứng dụng liên quan luôn được cập nhật các bản vá bảo mật mới nhất là rất quan trọng. Các giải pháp bao gồm:

- Sử dụng các công cụ tự động cập nhật: triển khai các giải pháp như kured để tự động quản lý việc khởi động lại node khi có bản vá bảo mật.
- Thực hiện các chính sách cập nhật định kỳ: đảm bảo rằng các thành phần của hệ thống được kiểm tra và cập nhật thường xuyên để giảm thiểu rủi ro bảo mật.

2.6. Sử dụng các công cụ bảo mật tích hợp

Ngoài các giải pháp trên, việc sử dụng các công cụ bảo mật tích hợp có thể giúp tăng cường bảo mật cho K8S một cách hiệu quả. Các công cụ này bao gồm:

- Kubernetes security benchmarks: áp dụng các tiêu chuẩn bảo mật từ các tổ chức như CIS (center for internet security) để đảm bảo rằng cấu hình K8S đáp ứng các yêu cầu bảo mật tối thiểu.

- Container image scanning: sử dụng các công cụ như clair hoặc trivy để quét và phát hiện các lỗ hổng bảo mật trong các image container trước khi triển khai.

2.7. Đào tạo và nâng cao nhận thức

Việc đào tạo nhân viên và nâng cao nhận thức về bảo mật là một phần không thể thiếu trong việc bảo vệ hệ thống K8S. Các chương trình đào tạo nên tập trung vào:

- Nguyên tắc bảo mật cơ bản: giúp nhân viên hiểu rõ các nguyên tắc bảo mật và cách áp dụng chúng trong môi trường K8S.
- Các kỹ thuật tấn công và phòng thủ: giúp nhân viên nhận diện các loại tấn công phổ biến và biết cách phản ứng kịp thời.

Tóm lại, việc đảm bảo và tăng cường bảo mật cho nền tảng Kubernetes đòi hỏi một chiến lược toàn diện, kết hợp nhiều giải pháp kỹ thuật và quản lý. Mỗi giải pháp đều đóng góp vào việc tạo nên một môi trường K8S an toàn, ổn định và đáng tin cậy cho VNPT Hà Nội trên hạ tầng đơn vị.

3. Mục đích nghiên cứu

Mục tiêu chính của đề tài này là xây dựng các giải pháp tăng cường bảo mật cho nền tảng Kubernetes (K8S) tại VNPT Hà Nội trên hạ tầng đơn vị. Cụ thể, các mục tiêu nghiên cứu bao gồm:

- Đánh giá hiện trạng bảo mật của K8S tại VNPT Hà Nội: phân tích các điểm mạnh và điểm yếu trong hệ thống bảo mật hiện tại.
- Xác định các yêu cầu bảo mật cụ thể: dựa trên nhu cầu và thách thức hiện tại để đề xuất các biện pháp bảo mật phù hợp.
- Đề xuất và triển khai các giải pháp bảo mật: xây dựng các giải pháp kỹ thuật và quản lý nhằm nâng cao mức độ bảo mật của K8S.
- Thử nghiệm và đánh giá hiệu quả của các giải pháp: kiểm tra tính khả thi và hiệu quả của các giải pháp bảo mật đã triển khai.
- Nâng cao nhận thức về bảo mật trong tổ chức: thiết lập các chương trình đào tạo và nâng cao nhận thức cho nhân viên về tầm quan trọng của bảo mật..

4. Đối tượng và phạm vi nghiên cứu

Đề tài tập trung nghiên cứu và xây dựng giải pháp bảo mật cho nền tảng Kubernetes (K8S) tại VNPT Hà Nội, cụ thể trên hạ tầng đơn vị. Phạm vi nghiên cứu bao gồm:

- Hệ thống Kubernetes hiện tại tại VNPT Hà Nội: phân tích cấu hình, quản lý quyền truy cập, bảo mật mạng nội bộ, quản lý thông tin quan trọng và các biện pháp giám sát hiện có.
- Các yếu tố bảo mật liên quan: cấu hình hệ thống, quản lý quyền truy cập, bảo mật mạng, quản lý thông tin quan trọng, giám sát và phát hiện xâm nhập, quản lý bản vá và cập nhật.
- Giải pháp bảo mật kỹ thuật và quản lý: đề xuất các công cụ, phương pháp và chính sách bảo mật phù hợp với môi trường hạ tầng đơn vị của VNPT Hà Nội.
- Thử nghiệm và đánh giá: xây dựng mô hình thử nghiệm trên hạ tầng đơn vị và đánh giá hiệu quả của các giải pháp bảo mật được triển khai.
- Nhân sự và nhận thức bảo mật: phân tích và đề xuất các chương trình đào tạo nhằm nâng cao nhận thức bảo mật cho nhân viêng.

5. Phương pháp nghiên cứu

Để đạt được mục tiêu nghiên cứu, đề tài này sẽ sử dụng các phương pháp nghiên cứu khoa học sau:

- Phân tích tài liệu: tổng hợp và phân tích các tài liệu liên quan đến bảo mật Kubernetes để xây dựng cơ sở lý thuyết và các giải pháp bảo mật phù hợp.
- Khảo sát và đánh giá hiện trạng: đánh giá cấu hình và các biện pháp bảo mật hiện tại của hệ thống Kubernetes tại VNPT Hà Nội, xác định vấn đề bảo mật cần khắc phục.
- Nghiên cứu định tính: thiết kế các giải pháp bảo mật kỹ thuật và quản lý dựa trên kết quả khảo sát và các thảo luận với các chuyên gia bảo mật.
- Phương pháp thực nghiệm: triển khai và thử nghiệm các giải pháp bảo mật trên môi trường thử nghiệm tại VNPT Hà Nội để kiểm tra hiệu quả của các giải pháp.
- Phân tích và đánh giá kết quả: phân tích dữ liệu từ các thử nghiệm để đánh giá hiệu quả của các giải pháp bảo mật và đưa ra các cải tiến cần thiết

II. Nội dung

Mở đầu

Lý do chọn đề tài

Mục đích nghiên cứu

Đối tượng và phạm vi nghiên cứu

Phương pháp nghiên cứu

Chương 1: Tổng quan về bảo mật trong Kubernetes

1.1. Giới thiệu về Kubernetes

- Khái niệm và thành phần cơ bản của K8S
- Lợi ích và ứng dụng của K8S trong quản lý container

1.2. Các mối đe dọa bảo mật cho Kubernetes

- Phân loại các mối đe dọa bảo mật
- Các vụ tấn công phổ biến vào K8S

1.3. Nguyên tắc bảo mật trong Kubernetes

- Chính sách bảo mật (security policies)
- Quản lý quyền truy cập (RBAC)
- Mã hóa dữ liệu và giao tiếp

1.4. Các tiêu chuẩn và khung bảo mật cho Kubernetes

- Cis Kubernetes benchmark
- Kubernetes Security Best Practices

Chương 2: Giải pháp bảo mật cho Kubernetes tại VNPT Hà Nội

2.1. Khảo sát yêu cầu bảo mật tại VNPT Hà Nội

- Đánh giá hiện trạng bảo mật K8S tại VNPT Hà Nội trên hạ tầng đơn vị
- Xác định các yêu cầu bảo mật cụ thể dựa trên nhu cầu và thách thức hiện tại

2.2. Đề xuất chi tiết các giải pháp bảo mật

2.2.1. Cấu hình và triển khai công cụ bảo mật

- Thiết lập RBAC
- Cấu hình network policies
- Sử dụng container image scanning Trivy

2.2.2. Quản lý thông tin quan trọng và cấu hình

- Sử dụng Kubernetes secrets
- Tích hợp với các hệ thống quản lý thông tin quan trọng bên ngoài

2.2.3. Giám sát và phát hiện xâm nhập

- Triển khai Prometheus và Grafana

- Sử dụng Falco cho hệ thống phát hiện xâm nhập

2.2.4. Bảo mật mạng nội bộ

- Áp dụng service mesh với Istio
- Thiết lập các chính sách mạng nghiêm ngặt trên hạ tầng đơn vị

2.2.5. Quản lý bản vá và cập nhật

- Sử dụng công cụ kured
- Thực hiện chính sách cập nhật định kỳ

Chương 3: Thử nghiệm và đánh giá

3.1. Xây dựng mô hình thử nghiệm

- Mô tả môi trường thử nghiệm trên hạ tầng đơn vị
- Các thành phần và công cụ được sử dụng trong mô hình

3.2. Xây dựng các kịch bản thử nghiệm

3.2.1. Thử nghiệm cấu hình và cài đặt công cụ bảo mật

Kiểm tra RBAC và network policies. Cài đặt công cụ Trivy.

3.2.2. Thử nghiệm quản lý thông tin quan trọng

Sử dụng Kubernetes Secrets và quản lý thông tin quan trọng cho hệ thống.

3.2.3. Thử nghiệm giám sát và phát hiện xâm nhập

Cài đặt công cụ giám sát Grafana, Prometheus và kiểm tra khả năng phát hiện và phản ứng của hệ thống giám sát.

3.2.4. Thử nghiệm bảo mật mạng nội bộ

Cài đặt công cụ Istio. Phần vùng mạng và đặt các policy cho hệ thống.

3.2.5. Thử nghiệm quản lý bản vá và cập nhật

Cập nhật bản và cho các node và cài đặt công cụ kured để thử nghiệm tính năng.

3.3. Đánh giá kết quả thử nghiệm

- Phân tích kết quả từng kịch bản thử nghiệm
- Đánh giá mức độ hiệu quả của các giải pháp bảo mật đã triển khai

3.4. Đề xuất cải tiến và phát triển trong tương lai

- Nhận diện các điểm mạnh và điểm yếu của giải pháp hiện tại
- Đề xuất các hướng phát triển và cải tiến để tăng cường bảo mật hơn nữa

III. Kết luận

Đề tài "xây dựng giải pháp tăng cường bảo mật cho nền tảng Kubernetes tại VNPT Hà Nội" nhằm mục tiêu phân tích hiện trạng bảo mật của K8S trên hạ tầng đơn vị, khảo sát các giải pháp bảo mật hiện có, và đề xuất những giải pháp phù hợp nhất để nâng cao mức độ bảo mật cho nền tảng này tại VNPT Hà Nội. Thông qua việc xây dựng và thử nghiệm các giải pháp, đề tài không chỉ giúp bảo vệ hệ thống hiện tại mà còn đóng góp vào việc phát triển bền vững và an toàn cho các ứng dụng và dịch vụ của VNPT trong tương lai. Đồng thời, nó cũng thúc đẩy việc nâng cao nhận thức về bảo mật trong toàn tổ chức, đảm bảo một môi trường làm việc an toàn và tin cậy hơn.

danh mục tài liệu tham khảo

[1] A. S. Bueno and a. Block, Kubernetes secrets management. Simon and schuster, 2023..

[2] E. Gkatziouras, r. Adams, and c. Xi, Kubernetes secrets handbook: design, implement, and maintain production-grade Kubernetes secrets management solutions. Packt publishing ltd, 2024

[3] Veeranjaneyulu veeri, " modern Kubernetes ingress solutions: an indepth comparison of contour and istio architecturess," [online]. Available: https://www.researchgate.net/profile/veeranjaneyulu-veeri/publication/385881420_modern_Kubernetes_ingress_solutions_an_in-_depth_comparison_of_contour_and_istio_architectures/links/6738d10968de5e5a3078e658/modern-Kubernetes-ingress-solutions-an-in-depth-comparison-of-contour-and-istio-architectures.pdf/. [accessed 2024].

[4] Sarp koksal 1,2, ferhat ozgur catak 3 , (senior member, ieee), and yaser dalveren 4, " flexible and lightweight mitigation framework for distributed denial-of-service attacks in container-based edge networks using Kubernetes," [online]. Available: https://ieeexplore.ieee.org/stamp/stamp.jsp?Tp=&arnumber=10755088/. [accessed 2024].

IV. Dự kiến kế hoạch thực hiện hoàn thành đề án

Stt	Nội dung	Dự kiến thời gian thực hiện
1	Nghiên cứu, chọn đề tài, xây dựng đề cương đề án	01/12/2024-09/12/2024

2	Nộp đề cương đề án	09/12/2024
3	Chương 1	15/12/2024-15/01/2025
4	Chương 2	16/01/2025-28/02/2025
5	Chương 3	01/03/2025-20/04/2025
6	Chỉnh sửa, hoàn thiện đề án	21/04/2025-01/06/2025
7	Nộp quyển đề án và hồ sơ bảo vệ đề án	06/2024

Ý kiến của
Người hướng dẫn khoa học

PGS.TS HOÀNG XUÂN DẬU

Người lập đề cương

VŨ TUẤN NHẬT

Duyệt của chủ tịch hội đồng

PGS.TS HOÀNG XUÂN DẬU