ĐẠI HỌC QUỐC GIA THÀNH PHỐ HỒ CHÍ MINH

TRƯỜNG ĐẠI HỌC CÔNG NGHỆ THÔNG TIN

KHOA MẠNG MÁY TÍNH VÀ TRUYỀN THÔNG

BÁO CÁO ĐỒ ÁN

MÔN LẬP TRÌNH KỊCH BẢN TỰ ĐỘNG HÓA CHO QUẢN TRỊ VÀ BẢO MẬT MẠNG

Đề tài:

CIS GOOGLE KUBERNETES ENGINE (GKE) AUTOPILOT BENCHMARK

Giảng viên hướng dẫn: Th.S. Trần Thị Dung

Lớp: NT542.Q11

Nhóm thực hiện: Nhóm 20

STT	Họ và tên	MSSV
1	Đinh Huỳnh Gia Bảo	22520101
2	Nguyễn Xuân Cường	22520178

THÀNH PHỐ HỒ CHÍ MINH, 2025

MỤC LỤC

DANH MỤC HÌNH ẢNH

s

DANH MỤC VIẾT TẮT

Số thứ tự	Chữ viết tắt	Ý nghĩa	Mô tả
1	GKE	Google Kubernetes Engine	Một dịch vụ quản lý Kubernetes của Google Cloud, mang đến một giải pháp cho việc triển khai, cân bằng tải và quản lý ứng dụng dựa trên container.
2	CIS	Center for Internet Security	Một tổ chức phi lợi nhuận ở Mỹ, chuyên tập trung vào việc nâng cao mức độ an toàn thông tin và khả năng phòng thủ mạng.
3	CLI	Command Line Interface	Phương pháp người dùng tương tác với hệ thống thông qua các lệnh dạng văn bản thay vì dùng giao diện đồ họa.
4	SDK	Software Developmen Kit	Gói công cụ phát triển phần mềm, bao gồm thư viện mã nguồn, trình biên dịch, trình gỡ lỗi, tài liệu, mẫu mã, và hướng dẫn
5	OS	Operating System	Là phần mềm hệ thống quản lý tài nguyên phần cứng và phần mềm của máy tính và cung cấp các dịch vụ chung cho các chương trình ứng dụng.
6	RBAC	Role-Based Access Control	Mô hình điều khiển truy cập trong đó quyền được gán cho các vai trò
7	KMS	Key Management Service	Dịch vụ tập trung quản lý vòng đời các khóa mã hóa trong hệ thống
8	IAM	Identity and Access Management	Tập hợp quy trình, công nghệ và chính sách để xác thực và ủy quyền

LỜI CẢM ƠN

Để hoàn thành được đồ án môn Lập trình kịch bản tự động hóa cho quản trị và bảo mật mạng này, Nhóm 20 chúng em xin gửi lời cảm ơn chân thành về sự chỉ dạy, hướng dẫn tận tình của cô ThS. Trần Thị Dung, giảng viên Khoa Mạng máy tính và Truyền thông, trường Đại học Công nghệ Thông tin – Đại học Quốc Gia Hồ Chí Minh.

Mặc dù trong quá trình làm đồ án, nhóm chúng em đã rất cố gắng, tuy nhiên cũng không tránh khỏi những thiếu sót. Chúng em hy vọng rằng sẽ nhận được những nhận xét, góp ý của cô về những vấn đề được triển khai trong bài báo cáo đồ án này, giúp chúng em có thể hoàn thiện và có những kinh nghiệm quý báu cho những đồ án tiếp theo.

Cuối cùng, chúng em xin kính chúc cô luôn dồi dào sức khỏe và thành công trong sự nghiệp giảng dạy cao quý.

Chúng em xin chân thành cảm ơn!

Thành phố Hồ Chí Minh, ngày 22 tháng 10 năm 2025

Nhóm 20

1. TỔNG QUAN

1.1. Giới thiệu

1.1.1 CIS và CIS Benchmark

Center for Internet Security, hay có tên viết tắt là **CIS,** là một tổ chức phi lợi nhuận với nhiệm vụ xây dựng các tiêu chuẩn bảo mật toàn cầu cho hạ tầng công nghệ thông tin. CIS tập trung vào việc cung cấp các hướng dẫn, công cụ và tiêu chuẩn giúp các tổ chức giảm thiểu rủi ro trong an ninh mạng, trong đó **CIS Benchmarks™** là một trong những bộ tiêu chuẩn nổi bật và được sử dụng rộng rãi nhất trong các hệ thống, nền tảng và dịch vụ đám mây.

CIS Benchmarks là tài liệu tập trung vào các cài đặt cấu hình kỹ thuật được sử dụng để duy trì hoặc tăng cường bảo mật cho công nghệ được đề cập. Các Benchmark này được thiết kế để trở thành một thành phần cốt lõi của một chương trình an ninh mạng toàn diện.

Quá trình phát triển các CIS Benchmark được thực hiện thông qua quy trình đánh giá đồng thuận với sự tham gia của một cộng đồng các chuyên gia chủ đề toàn cầu. Quá trình này kết hợp kinh nghiệm thực tế với thông tin dựa trên dữ liệu để tạo ra hướng dẫn mang tính quy tắc cụ thể theo công nghệ nhằm hỗ trợ người dùng bảo mật môi trường của họ.

1.1.2 CIS Google Kubernetes Engine (GKE) Autopilot Benchmark

Cuốn **CIS Google Kubernetes Engine (GKE) Autopilot Benchmark v1.2.0**, được phát hành vào tháng 6 năm 2025, là tài liệu hướng dẫn cấu hình bảo mậ t chuyên biệt cho nền tảng Google Kubernetes Engine (GKE) ở chế độ Autopilot. Tài liệu này tập trung vào những thiết lập mà người dùng cuối có thể kiểm soát để đảm bảo tính bảo mật, tính tuân thủ, và khả năng kiểm toán khi vận hành cụm Kubernetes trên Google Cloud.

Trong Benchmark, các khuyến nghị được chia thành hai cấp độ:

- **Level 1**: Bao gồm các thiết lập **bảo mật cơ bản**, mang tính **thiết thực** và **dễ áp dụng**, nhằm đảm bảo an toàn mà không ảnh hưởng đáng kể đến hiệu năng và tính ổn định của hệ thống. Đây là cấp độ phù hợp cho phần lớn môi trường doanh nghiệp hoặc hệ thống sản xuất tiêu chuẩn.

- **Level 2**: Bao gồm các thiết lập **nâng cao** và **chuyên sâu hơn**, hướng đến việc tăng cường mức độ bảo mật cho các hệ thống đòi hỏi độ tin cậy cao hoặc có dữ liệu nhạy cảm. Một số

khuyến nghị ở Level 2 có thể yêu cầu thay đổi sâu về cấu hình hoặc ảnh hưởng đến khả năng vận hành, nên cần được xem xét kỹ trước khi áp dụng.

Nhờ sự phân cấp rõ ràng này, người quản trị có thể lựa chọn áp dụng Benchmark phù hợp với mức độ rủi ro, quy mô và yêu cầu bảo mật của tổ chức, từ đó xây dựng nên một hệ thống GKE an toàn, nhất quán và tuân thủ các chuẩn về an ninh của quốc tế.

1.2. Nội dung Benchmark

CIS GKE Autopilot Benchmark được cấu trúc xoay quanh hai nhóm nội dung trọng tâm: **Policies** và **Managed Services**. Hai phần này bao quát toàn bộ các khía cạnh bảo mật quan trọng của một cụm Kubernetes trong môi trường Autopilot, từ việc kiểm soát truy cập nội bộ đến việc quản lý an toàn các dịch vụ đám mây tích hợp. Nhờ cách phân tách minh bạch này, người quản trị có thể dễ dàng triển khai, đánh giá và duy trì cấu hình bảo mật cho từng lớp của hệ thống.

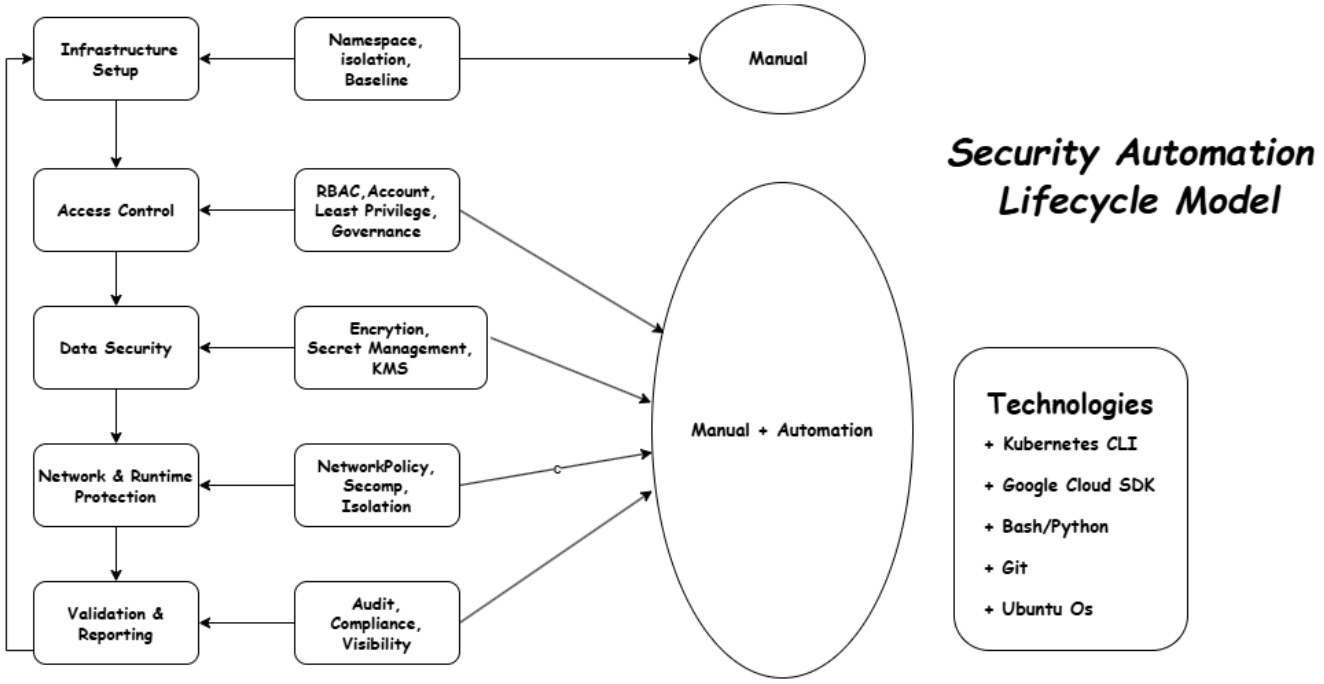
1.2.1 Policies

Phần này tập trung vào các chính sách bảo mật trong cụm GKE Autopilot, bao gồm kiểm soát truy cập dựa trên vai trò người dùng (RBAC), quản lý tài khoản dịch vụ, chuẩn bảo mật cho Pod, cấu hình mạng, và quản lý Secrets. Các chính sách được thiết kế nhằm đảm bảo quyền truy cập tối thiểu, cô lập tài nguyên, và ngăn chặn các hành vi cố gắng xâm nhập trái phép trong môi trường Kubernetes. Ngoài ra, phần này cũng đề cập đến các cơ chế như Admission Control và Namespace để tăng cường tính an toàn cho toàn bộ cụm.

1.2.2 Managed Services

Chương này tập trung vào các dịch vụ được quản lý trong GKE Autopilot, bao gồm Image Registry, IAM, Cloud KMS, Network, Authentication, Storage, và các cấu hình cụm khác. Mục tiêu là hướng dẫn người dùng các phương pháp đảm bảo an toàn cho các thành phần tích hợp với Google Cloud, chẳng hạn như bật quét lỗ hổng Image, mã hóa Secrets bằng Cloud KMS, hay kiểm soát quyền truy cập IAM.

2. PHƯƠNG PHÁP



Hình 1. Mô hình tổng quan đồ án

Mô hình này đặc tả kiến trúc 5 tầng của hệ thống bảo mật tự động cho GKE Autopilot, được thiết kế dựa trên các nhóm kiểm soát trong bộ tiêu chuẩn CIS Benchmark thuộc Level 1.

Mỗi tầng đại diện cho một giai đoạn bảo mật cụ thể trong vòng đời tự động hoá: từ khâu chuẩn bị hạ tầng, kiểm soát truy cập, bảo vệ dữ liệu, bảo mật mạng và runtime, cho đến xác thực và báo cáo kết quả tuân thủ.

Mô hình này kết hợp hài hòa giữa cấu hình thủ công và tự động hóa bằng kịch bản, tạo nên sự cân bằng giữa tính trực quan khi thao tác thủ công và nâng cao hiệu suất của quy trình tự động. Các công nghệ được sử dụng gồm Kubernetes CLI, Google Cloud SDK, Bash/Python, Git, và Ubuntu OS, hỗ trợ cho quá trình kiểm tra, khắc phục, và báo cáo tuân thủ bảo mật.

3. TRIỂN KHAI

TÀI LIỆU THAM KHẢO

PHỤ LỤC

Phân công

STT	Họ và tên	Nhiệm vụ	Tỉ lệ %
1	Đinh Huỳnh Gia Bảo		Nghiêm túc thực hiện công việc và hoàn thành đúng tiến độ: 100%
2	Nguyễn Xuân Cường		Nghiêm túc thực hiện công việc và hoàn thành đúng tiến độ: 100%

NHẬN XÉT CỦA GIẢNG VIÊN

.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....