

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

MỤC LỤC.....	2
DANH MỤC HÌNH ẢNH	4
DANH MỤC VIẾT TẮT.....	5
LỜI CẢM ƠN.....	7
1. TỔNG QUAN	8
1.1. Giới thiệu.....	8
1.1.1 CIS và CIS Benchmark	8
1.1.2 CIS Google Kubernetes Engine (GKE) Autopilot Benchmark	8
1.2. Nội dung Benchmark	9
1.2.1 Policies	9
1.2.1.1 Phân quyền dựa trên vai trò (RBAC) và Tài khoản dịch vụ (Service Account).....	9
1.2.1.4 Tiêu chuẩn bảo mật Pod	12
1.2.1.3 Các chính sách tổng quát	12
1.2.2 Managed Services.....	12
1.2.2.1 Mạng lưới trong cụm (Cluster Networking)	13
2. PHƯƠNG PHÁP	13
2.1 Manual	13
2.2 Automation.....	13
3. TRIỂN KHAI.....	14
3.1 Kế hoạch triển khai.....	14
3.1.1 Tạo cụm GKE.....	14
3.1.1.1 Phương pháp Manual	14
3.1.1.2 Phương pháp Automation	19
3.1.2 Công việc chi tiết.....	19
3.2 Manual.....	21
3.3 Automation.....	21
TÀI LIỆU THAM KHẢO	23

PHỤ LỤC	25
NHẬN XÉT CỦA GIẢNG VIÊN.....	26

DANH MỤC HÌNH ẢNH

DANH MỤC VIẾT TẮT

CIS GOOGLE KUBERNETES ENGINE (GKE) AUTOPILOT BENCHMARK

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 vẫn 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 mật 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 có 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.

1.2.1.1 Phân quyền dựa trên vai trò (RBAC) và Tài khoản dịch vụ (Service Account)

Ensure that the cluster-admin role is only used where required (Automated):

- Dịch: Đảm bảo vai trò cluster-admin chỉ được sử dụng khi cần thiết (Tự động hóa)
- Ý nghĩa: Vai trò *cluster-admin* cung cấp đặc quyền quản trị cao nhất trong toàn bộ cụm Kubernetes. Mục đích của việc hạn chế sử dụng vai trò này giúp giảm thiểu nguy cơ lạm dụng quyền và ngăn chặn các tác động không mong muốn đến hệ thống. Các tài khoản chỉ nên được gán *cluster-admin* khi thực sự cần thiết cho các hoạt động quản trị chủ yếu.

Minimize access to secrets (Automated):

- Dịch: Giảm thiểu quyền truy cập vào secrets.
- Ý nghĩa: Secrets chứa thông tin nhạy cảm như token, khóa API hoặc thông tin xác thực của

ứng dụng, do đó cần được bảo vệ và kiểm soát chặt chẽ. Giới hạn quyền truy cập vào Secrets giúp tránh nguy cơ rò rỉ dữ liệu và ngăn chặn khả năng leo thang đặc quyền. Chỉ các tài khoản hoặc workload được ủy quyền rõ ràng mới nên có quyền đọc Secret.

Minimize wildcard use in Roles and ClusterRoles (Automated):

- **Dịch:** Giảm thiểu việc sử dụng ký tự đại diện (wildcard) trong Roles và ClusterRoles.
- **Ý nghĩa:** Kubernetes Roles (vai trò) và ClusterRoles (vai trò cấp cụm) cung cấp quyền truy cập vào các tài nguyên dựa trên các tập hợp đối tượng và hành động có thể thực hiện được gán cho các đối tượng đó. Có thể đặt một trong hai thành ký tự đại diện “*” (wildcard), khớp với tất cả các mục. Khi loại bỏ hoặc hạn chế wildcard giúp đảm bảo rằng từng quyền được ủy quyền một cách cụ thể và có thể kiểm soát được. Điều này cũng hỗ trợ công việc kiểm toán và giám sát an ninh một cách dễ dàng hơn.

Ensure that default service accounts are not actively used (Automated):

- **Dịch:** Đảm bảo rằng các tài khoản dịch vụ mặc định không được sử dụng một cách chủ động.
- **Ý nghĩa:** Service Account mặc định thường đi kèm các quyền không thật sự cần thiết đối với nhiều workload. Không nên sử dụng Service Account mặc định giúp bảo đảm rằng mỗi ứng dụng đều được gán quyền tối thiểu cần thiết. Điều này tăng tính minh bạch và độ chính xác khi đánh giá quyền hạn của từng workload..

Ensure that Service Account Tokens are only mounted where necessary (Automated):

- **Dịch:** Đảm bảo rằng Service Account Token chỉ được gắn kết khi cần thiết.
- **Ý nghĩa:** Service Account Token chỉ nên được gắn vào Pod khi workload cần tương tác trực tiếp với API Server. Việc gắn token không cần thiết làm tăng rủi ro token bị bại lộ hoặc bị lạm dụng bởi các phần mềm độc hại. Giảm bớt token mount giúp tăng cường mức độ cô lập và an toàn cho Pod.

Avoid use of system:masters group (Automated):

- Dịch: Tránh sử dụng nhóm system:masters.
- Ý nghĩa: Nhóm system:masters được Kubernetes mặc định cấp quyền truy cập đầy đủ vào API mà không bị giới hạn bởi RBAC. Việc hạn chế sử dụng nhóm này giúp chúng ta giảm thiểu khả năng truy cập vượt mức và tăng tính an toàn, dễ dàng kiểm soát trên toàn cùm. Chỉ có các tài khoản quản trị đặc biệt mới nên được cẩn nhắc gán vào nhóm này.

Limit use of the Bind, Impersonate and Escalate permissions in the Kubernetes cluster (Manual):

- Dịch: Giới hạn việc sử dụng quyền Bind, Impersonate và Escalate trong Kubernetes cluster.
- Ý nghĩa: ClusterRole và các Role có quyền Impersonate (mạo danh), Bind (liên kết) hoặc Escalate (leo thang) không nên được cấp trừ khi có yêu cầu nghiêm ngặt. Chỉ nên gán các quyền này khi có yêu cầu vận hành đặc biệt và được giám sát một cách chặt chẽ. Kiểm soát cẩn thận nhóm quyền này là cần thiết để bảo vệ hệ thống khỏi các hành vi leo thang đặc quyền.

Avoid bindings to system:anonymous (Automated):

- Dịch: Tránh các liên kết (bindings) tới system:anonymous.
- Ý nghĩa: Người dùng system:anonymous đại diện cho các yêu cầu không cần xác thực và không nên được gán bất kỳ quyền truy cập nào cho người dùng này. Hạn chế binding tới tài khoản này giúp ngăn chặn truy cập trái phép vào API Server. Đây là biện pháp nền tảng nhằm duy trì mức bảo mật tối thiểu của cùm.

Avoid non-default bindings to system:unauthenticated (Automated):

- Dịch: Tránh cấu hình các Binding không mặc định đối với nhóm system:unauthenticated
- Ý nghĩa: Nhóm system:unauthenticated không yêu cầu xác thực danh tính nên không được cấp thêm quyền ngoài cấu hình mặc định. Việc bổ sung binding cho nhóm này làm tăng nguy cơ truy cập bất hợp pháp. Các namespace và ứng dụng không nên phụ thuộc vào bất kỳ quyền nào thuộc nhóm này.

Avoid non-default bindings to system:authenticated (Automated)

- Dịch: Tránh cấu hình các Binding không mặc định đối với nhóm system:authenticated
- Ý nghĩa: Nhóm system:authenticated bao gồm tất cả người dùng đã xác thực và do đó có phạm vi rất rộng. Không nên gán ClusterRole cho toàn bộ nhóm này trừ các trường hợp thực sự cần thiết. Việc giới hạn quyền đảm bảo rằng từng tài khoản chỉ có quyền phù hợp với vai trò được xác định.

1.2.1.4 Tiêu chuẩn bảo mật Pod

Ensure that the cluster enforces Pod Security Standard Baseline profile or stricter for all namespaces. (Manual):

- Dịch: Đảm bảo cụm áp dụng và thực thi hồ sơ Pod Security Standard Baseline hoặc nghiêm ngặt hơn cho tất cả các namespace.
- Ý nghĩa: Pod Security Standard Baseline cung cấp bộ quy tắc bảo mật tối thiểu để ngăn chặn cấu hình Pod không an toàn. Áp dụng quy tắc Baseline (hoặc cao hơn) cho toàn bộ namespace giúp giảm thiểu các tình huống rủi ro như chạy container đặc quyền hoặc mount volume mang tính chất nhạy cảm. Đây là bước bắt buộc để duy trì mức an toàn nhất quán cho toàn cụm.

1.2.1.3 Các chính sách tổng quát

Create administrative boundaries between resources using namespaces (Manual):

- Dịch: Tạo ranh giới quản trị giữa các tài nguyên bằng cách sử dụng namespaces.
- Ý nghĩa: Namespaces cho phép phân tách tài nguyên một cách logic trong cụm, giúp kiểm soát quyền truy cập và giới hạn phạm vi quản trị. Việc sử dụng namespaces làm tăng tính cô lập giữa ứng dụng và hỗ trợ triển khai mô hình RBAC chi tiết hơn. Đây là một trong những phương pháp quan trọng, an toàn để đảm bảo cấu trúc quản lý nhất quán và an toàn.

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.

1.2.2.1 Mạng lưới trong cụm (Cluster Networking)

Enable VPC Flow Logs and Intranode Visibility:

- **Dịch:** Bật VPC Flow Logs và khả năng quan sát lưu lượng nội bộ giữa các node.
- **Ý nghĩa:** VPC Flow Logs cung cấp khả năng giám sát lưu lượng mạng để phục vụ việc phân tích, điều tra và đảm bảo tính an ninh. Intranode Visibility cho phép quan sát lưu lượng nội bộ giữa các Pod trong cùng node, đảm bảo không có lưu lượng bị bỏ sót. Kích hoạt cả hai tính năng giúp tăng cường khả năng giám sát và đáp ứng sự cố mạng.

2. PHƯƠNG PHÁP

2.1 Manual

Một số yêu cầu Level 1 cần được kiểm tra hoặc đánh giá bằng nhận thức, không thể tự động hóa hoàn toàn. Đây là những mục yêu cầu quản trị viên xác minh đúng sai dựa trên thực trạng vận hành.

Sử dụng Google Cloud SDK Shell để:

- Rà soát quyền truy cập đặc biệt như Bind, Impersonate, Escalate.
- Kiểm tra namespace, phân quyền RBAC, cấu trúc tài nguyên và việc sử dụng workload.
- Xác minh thủ công bằng các lệnh tương tác với cụm Kubernetes như kubectl get, kubectl describe, và kiểm tra log để bảo đảm không có cấu hình vượt mức hoặc sử dụng sai mục đích.
- So sánh thực trạng hệ thống với yêu cầu Level 1 để xác định tuân thủ.

2.2 Automation

Phương pháp tự động được áp dụng cho các khuyến nghị có thể kiểm soát thông qua cấu hình hệ thống, công cụ DevOps hoặc các dịch vụ tích hợp sẵn của GKE. Mục tiêu của phương pháp này là đảm bảo khả năng “tái tạo cấu hình” và hạn chế lỗi do thao tác thủ công.

Các phương pháp Automation :

- Thiết lập cấu hình bảo mật bằng kubectl, gcloud, YAML manifest hoặc Terraform.
- Sử dụng các nhãn (label), chính sách mặc định và thông số cấu hình để áp dụng Pod Security, RBAC, và Service Account theo yêu cầu Level 1.

- Bật các tính năng giám sát (ví dụ: VPC Flow Logs, Intranode Visibility) trực tiếp bằng gcloud hoặc UI.
- Tự động hóa quá trình kiểm tra bằng cách công cụ như kube-bench để đối chiếu với tiêu chí của CIS Level 1.

3. TRIỂN KHAI

3.1 Kế hoạch triển khai

3.1.1 Tạo cụm GKE

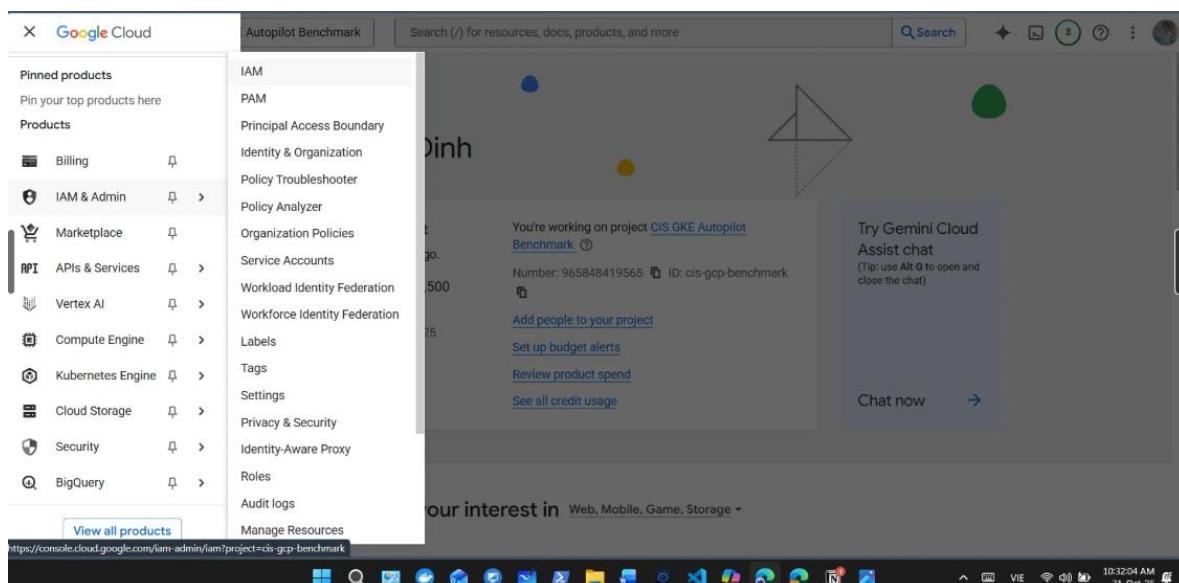
3.1.1.1 Phương pháp Manual

Tạo project

- Đăng nhập tài khoản GCP ở đường dẫn sau: [Google Cloud Platform](#)
- Tạo project mới có tên CIS GKE Autopilot Benchmark

Quản lý quyền người dùng:

- Khi tạo một project mới trong Google Cloud, tài khoản tạo project sẽ mặc định có vai trò Owner, tức là sở hữu toàn quyền quản trị (bao gồm quản lý tài nguyên, phân quyền, và cấu hình bảo mật).
- Để thêm thành viên mới vào project, thực hiện như sau:
 - Nhấn vào biểu tượng  (Navigation menu) ở góc trên bên trái màn hình.
 - Chọn **IAM & Admin** → **IAM** để mở trang quản lý thành viên và phân quyền truy cập cho project.



- Chọn Grant Access để tiến hành cấp quyền truy cập cho thành viên mới.
 - Nhập các thông tin cần thiết như sau:

Principal [?](#) xuancuongchywiz@gmail.com

Project CIS GKE Autopilot Benchmark

Ask AI | [Comment](#) [Share](#) [Download](#) [Edit](#)

Assign roles

Roles are composed of sets of permissions and determine what the principal can do with this resource. [Learn more](#)

Role	IAM condition (optional) ?	Action
Dev Ops	+ Add IAM condition	Delete
Enables DevOps users to build and deploy applications, create, manage and perform administrative tasks on associated GCP resources		
Kubernetes Engine Develop...	+ Add IAM condition	Delete
Full access to Kubernetes API objects inside Kubernetes Clusters.		

[+ Add another role](#)

[Help me choose roles](#)

[Save](#) [Test changes](#) [Cancel](#)

- Principal:
 - Là đối tượng được cấp quyền truy cập (user, service account, hoặc group).
 - Ở đây: xuancuongchwywiz1@gmail.com chính là user cá nhân đang được phân quyền.
 - Project:
 - Là phạm vi áp dụng quyền (scope).
 - Mọi quyền gán ở đây áp dụng cho toàn bộ project CIS GKE Autopilot Benchmark.
 - Bao gồm các dịch vụ trong project: GKE, IAM, Compute, Storage, v.v.
 - Assign Roles:
 - Là danh sách các vai trò (IAM Roles) mà principal được gán.
 - Mỗi role chứa tập quyền (permissions) xác định hành động được phép thực hiện.
 - Một principal có thể có nhiều role cùng lúc, chính vì thế quyền sẽ được **cộng dồn**.
 - ◆ ***Role 1: DevOps***
 - Cho phép build, deploy và quản lý ứng dụng trên GCP.
 - Bao gồm quyền thao tác với: Cloud Build, Cloud Deploy, Artifact Registry, Compute Engine, Cloud Run, Cloud Storage (liên quan deploy), thích hợp cho DevOps Engineer hoặc CI/CD pipeline.

◆ ***Role 2: Kubernetes Engine Developer***

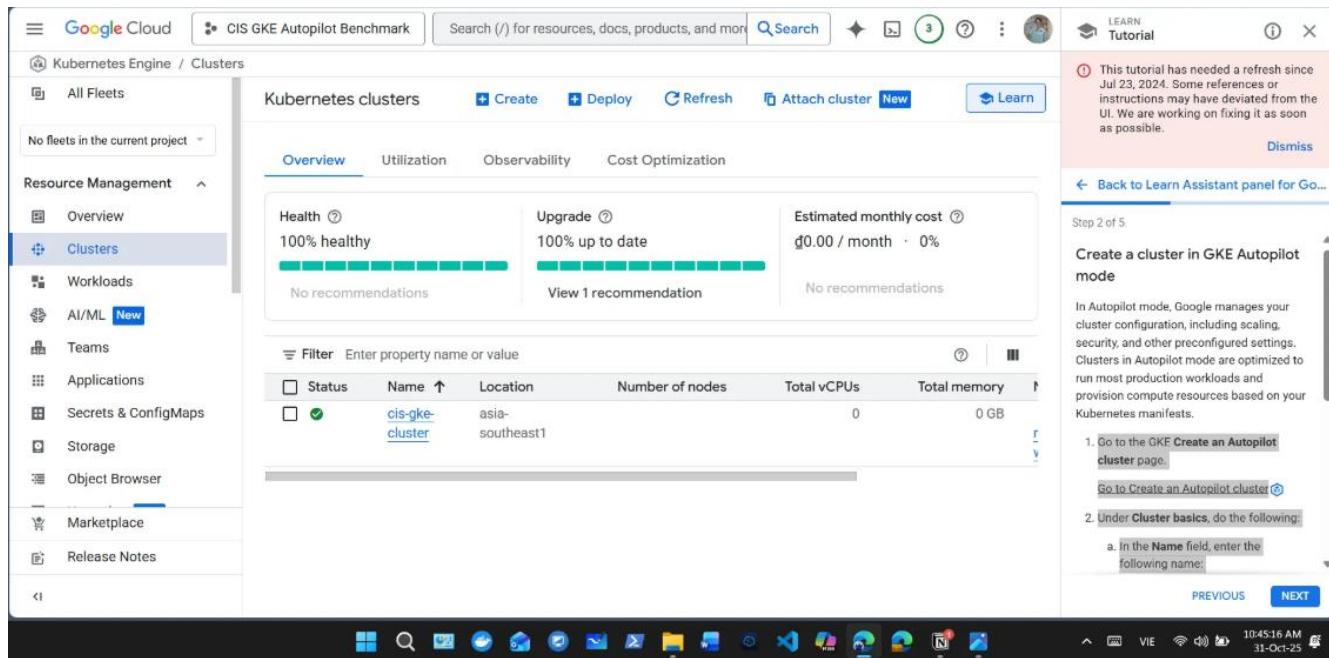
- Cung cấp đầy đủ quyền truy cập với Kubernetes API objects trong cluster (pods, deployments, services, ...).
- Cho phép thao tác tài nguyên trong GKE nhưng không tạo/xóa cluster.
- Thích hợp cho developer hoặc operator trong môi trường GKE.

• IAM Condition (Optional)

- Cho phép thêm điều kiện ràng buộc khi cấp quyền:
 - Theo thời gian (hiệu lực đến ngày X).
 - Theo địa chỉ IP (chỉ cho phép từ IP nội bộ).
 - Theo resource attribute (ví dụ: chỉ cho resource có label env=prod).
- Nếu không có điều kiện, quyền có hiệu lực toàn bộ, không giới hạn.

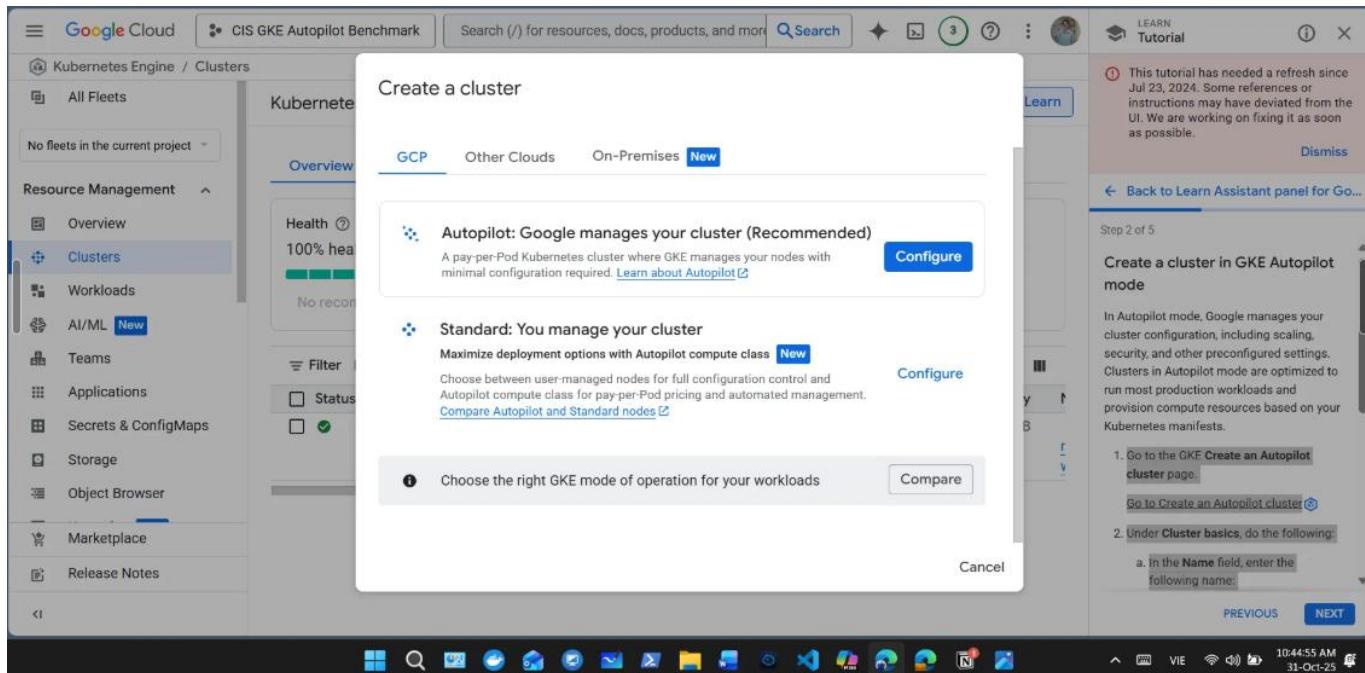
Tạo cụm GKE

- Mở menu  ở góc trái giao diện Google Cloud Console, chọn Kubernetes Engine.
- Chọn dự án Google Cloud sẽ triển khai cụm GKE (nếu có sẵn): CIS GKE Autopilot Benchmark. Đảm bảo Kubernetes API đã được kích hoạt trước khi tiếp tục.

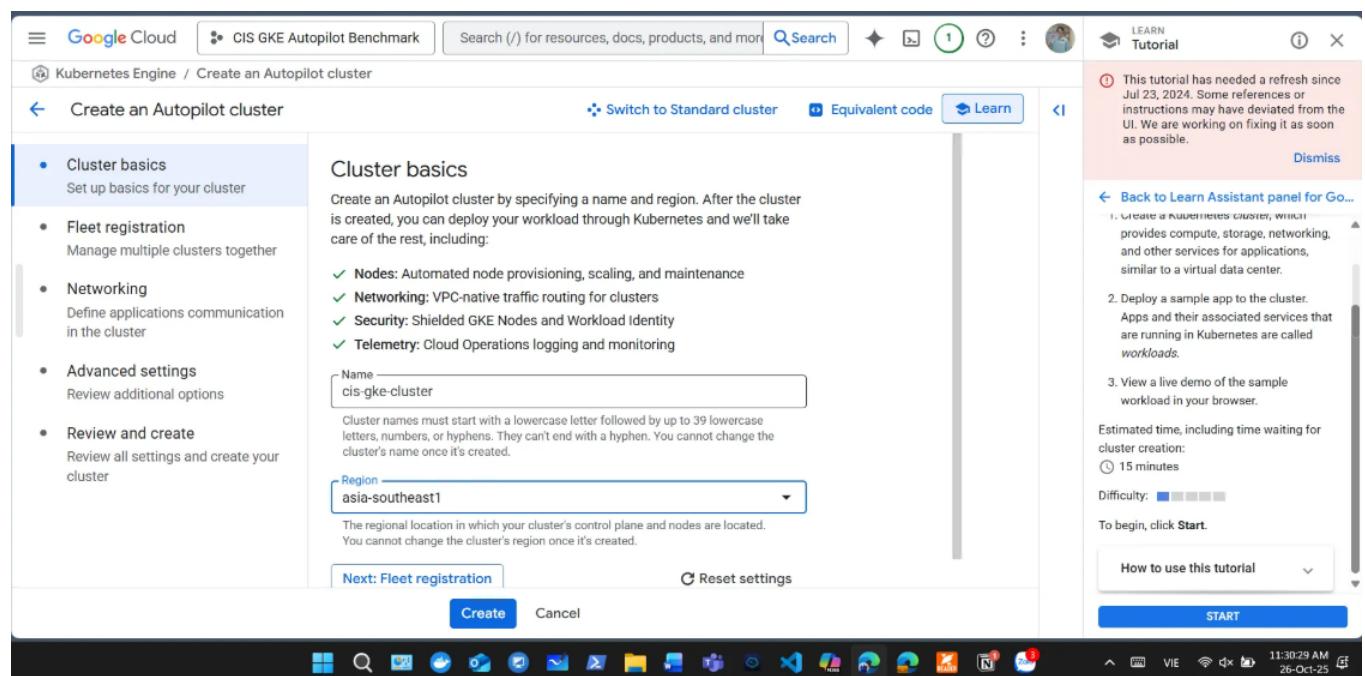


The screenshot shows the Google Cloud Console interface for managing Kubernetes clusters. On the left, there's a sidebar with 'All Fleets' and 'Resource Management' sections, with 'Clusters' currently selected. The main content area is titled 'Kubernetes clusters' and shows a single cluster named 'cis-gke-cluster'. The cluster status is '100% healthy' and '100% up to date'. It also shows 'Estimated monthly cost' at '\$0.00 / month' and '0%' usage. Below the cluster details, there's a table with columns for Status, Name, Location, Number of nodes, Total vCPUs, and Total memory. The cluster 'cis-gke-cluster' is listed with a green checkmark in the Status column. To the right of the main content, there's a 'Learn' panel titled 'Create a cluster in GKE Autopilot mode'. It includes a note about the tutorial being outdated, a 'Dismiss' button, and a 'Back to Learn Assistant panel for Go...' link. The panel then lists steps to create a cluster, with the first step being 'Go to the GKE Create an Autopilot cluster page'.

- Trong giao diện GKE, chọn mục **Overview** trong thanh menu để bắt đầu tạo cụm GKE. Nhấn **Create → Autopilot: Google manages your cluster (Recommended)** để tạo cụm → Chọn **Configure**.



- Trong trường **Name**, nhập tên cụm: cis-gke-cluster. Trong trường **Region**, chọn vị trí triển khai: asia-southeast1 (Singapore).



- Giữ nguyên các giá trị mặc định khác trong phần Cluster basics. Nhấn **Create** để bắt đầu quá trình tạo cụm GKE Autopilot.

- Thông tin bổ sung hiển thị trong giao diện:
 - **Nodes:** Tự động cung cấp, mở rộng và bảo trì node.
 - **Networking:** Hỗ trợ định tuyến VPC-native.
 - **Security:** Bật Shielded GKE Nodes và Workload Identity.
 - **Telemetry:** Tích hợp Cloud Operations để thu thập log và giám sát.
- Sau khi hoàn tất, giao diện sẽ hiển thị tiến trình **Autopilot quản lý cụm** (Configure → Deploying → Health checks), và kết quả cuối cùng là trang **Overview** của cụm GKE đã tạo.

This screenshot shows the Google Cloud Kubernetes Engine Cluster details page for 'cis-gke-cluster'. The cluster status is 'Running' in 'Autopilot' mode, located in the 'asia-southeast1' region with an endpoint of 34.126.153.144. The 'Overview' tab is selected. A sidebar on the left shows the 'Clusters' section with 'hello-world-cluster' listed. A 'Learn Tutorial' panel on the right provides step-by-step instructions for creating the cluster.

- Đây là thông tin tổng quát của cụm:

This screenshot shows the Google Cloud Kubernetes Engine Clusters page. The 'Overview' tab is selected, displaying the health of the clusters (100% healthy), upgrade status (100% up to date), and estimated monthly cost (No recommendations). A table lists the cluster 'cis-gke-cluster' with details like Name, Location, Number of nodes, Total vCPUs, and Total memory. A sidebar on the left shows the 'Clusters' section with 'hello-world-cluster' listed. A 'Learn Tutorial' panel on the right provides step-by-step instructions for creating the cluster.

3.1.1.2 Phương pháp Automation

3.1.2 Công việc chi tiết

Mục benchmark	3.1: Manual	3.2 :Automated
4.1.1: Ensure that the cluster-admin role is only used where required (Automated) - Đảm bảo vai trò cluster-admin chỉ được sử dụng khi cần thiết (Tự động hóa)		<ul style="list-style-type: none"> Kiểm tra các RoleBinding và ClusterRoleBinding để xác định nơi cấp quyền cluster-admin. Xóa hoặc điều chỉnh các binding không cần thiết bằng YAML hoặc lệnh kubectl delete/patch. Xác nhận lại sau cấu hình bằng kubectl get clusterrolebindings để đảm bảo chỉ còn các binding cần thiết.
4.1.2 : Minimize access to secrets (Automated) - Giảm thiểu quyền truy cập vào secrets		<ul style="list-style-type: none"> Xuất Role/ClusterRole và lọc quyền truy cập secrets. Điều chỉnh YAML để giảm quyền. Kiểm tra lại bằng kubectl hoặc grep.
4.1.3 : Minimize wildcard use in Roles and ClusterRoles (Automated) - Giảm thiểu việc sử dụng ký tự đại diện (wildcard) trong Roles và ClusterRoles		<ul style="list-style-type: none"> Tìm quyền có wildcard trong YAML. Sửa YAML để thay * bằng API/verb cụ thể. Kiểm tra lại role sau chỉnh sửa.
4.1.4 : Ensure that default service accounts are not actively used (Automated) - Đảm bảo rằng các tài khoản dịch vụ mặc định không được sử dụng một cách chủ động		<ul style="list-style-type: none"> Kiểm tra Pod dùng default SA. Set automountServiceAccountToken=false hoặc chỉ định SA riêng. Kiểm tra lại Pod sau khi cấu hình.

4.1.5 : Ensure that Service Account Tokens are only mounted where necessary (Automated) - Đảm bảo rằng Mã thông báo Tài khoản Dịch vụ chỉ được gắn kết khi cần thiết		<ul style="list-style-type: none"> Kiểm tra automountServiceAccountToken. Update Deployment để tắt mount token. Xác nhận Pod sau triển khai.
4.1.6 : Avoid use of system:masters group (Automated) - Tránh sử dụng nhóm system:masters		<ul style="list-style-type: none"> Kiểm tra user/credential đang thuộc nhóm này. Xóa RoleBinding gắn với system:masters. Kiểm tra lại bằng kubectl auth.
4.1.7 : Limit use of the Bind, Impersonate and Escalate permissions in the Kubernetes cluster (Manual) - Giới hạn việc sử dụng quyền Bind, Impersonate và Escalate trong Kubernetes cluster	<ul style="list-style-type: none"> Kiểm tra Role/ClusterRole có quyền nhạy cảm. Dánh giá mục đích cấp quyền. Thu hồi hoặc chỉnh sửa quyền theo thực tế vận hành. 	
4.1.8 : Avoid bindings to system:anonymous (Automated) - Tránh các liên kết (bindings) tới system:anonymous		<ul style="list-style-type: none"> Tìm các bindings system:anonymous. Xóa hoặc sửa rolebinding. Kiểm tra lại bằng RBAC query.
4.1.9 : Avoid non-default bindings to system:unauthenticated (Automated) – Tránh các liên kết tới system:unauthenticated		<ul style="list-style-type: none"> Tìm binding liên quan nhóm này. Gỡ bỏ binding không mặc định. Kiểm tra lại danh sách RBAC.
4.1.10 : Avoid non-default bindings to system:authenticated (Automated) - Tránh các liên kết tới system:authenticated		<ul style="list-style-type: none"> Tìm binding có phạm vi rộng cho system:authenticated. Loại bỏ binding không cần thiết.

		<ul style="list-style-type: none"> Xác nhận lại cấu hình RBAC.
4.2.1 : Ensure that the cluster enforces Pod Security Standard Baseline profile or stricter for all namespaces. (Manual) - Đảm bảo rằng cluster tuân thủ Tiêu chuẩn Bảo mật Pod hoặc nghiêm ngặt hơn cho tất cả các namespace	<ul style="list-style-type: none"> Kiểm tra nhãn PSS của từng namespace. Đánh giá mức độ phù hợp với Baseline. Điều chỉnh namespace hoặc workload theo yêu cầu. 	
4.6.1 : Create administrative boundaries between resources using namespaces (manual) - Tạo ranh giới hành chính giữa các tài nguyên bằng cách sử dụng namespaces	<ul style="list-style-type: none"> Kiểm tra danh sách namespace. Kiểm tra workload trong default. Kiểm tra RBAC theo namespace để đánh giá phân tách. Điều chỉnh lại cấu trúc namespace nếu cần. 	
5.4.1 : Enable VPC Flow Logs and Intranode Visibility (Automated) – Bật nhật ký luồng VPC và hiển thị nội bộ node		<ul style="list-style-type: none"> Kiểm tra trạng thái Flow Logs. Bật Flow Logs bằng gcloud. Bật Intranode Visibility. Kiểm tra lại sau cấu hình.

3.2 Manual

3.3 Automation

TÀI LIỆU THAM KHẢO

PHỤ LỤC

Bảng 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