

1. Kubernetes Cluster Created

The screenshot shows the Google Cloud Console interface for a Kubernetes Engine cluster. The left sidebar contains navigation options like Clusters, Workloads, Services & Ingress, Applications, Secrets & ConfigMaps, Storage, Object Browser, Migrate to Containers, Backup for GKE, and Security Posture. The main panel displays the details for 'autopilot-cluster-1'.

Cluster basics

Property	Value	Actions
Name	autopilot-cluster-1	
Location type	Regional	
Region	us-central1	
Default node zones	us-central1-b, us-central1-c, us-central1-f, us-central1-a	
Release channel	Regular channel	UPGRADE AVAILABLE
Version	1.27.3-gke.100	
External endpoint	34.172.133.62	Show cluster certificate
Internal endpoint	10.128.0.2	Show cluster certificate

Automation

Property	Value	Actions
Maintenance window	Any time	
Maintenance exclusions	None	

2. Kubernetes Cluster and kubectl installed and configured.

The screenshot shows the Google Cloud Console interface for the 'Kubernetes clusters' overview. The left sidebar is the same as in the first screenshot. The main panel shows a table of clusters.

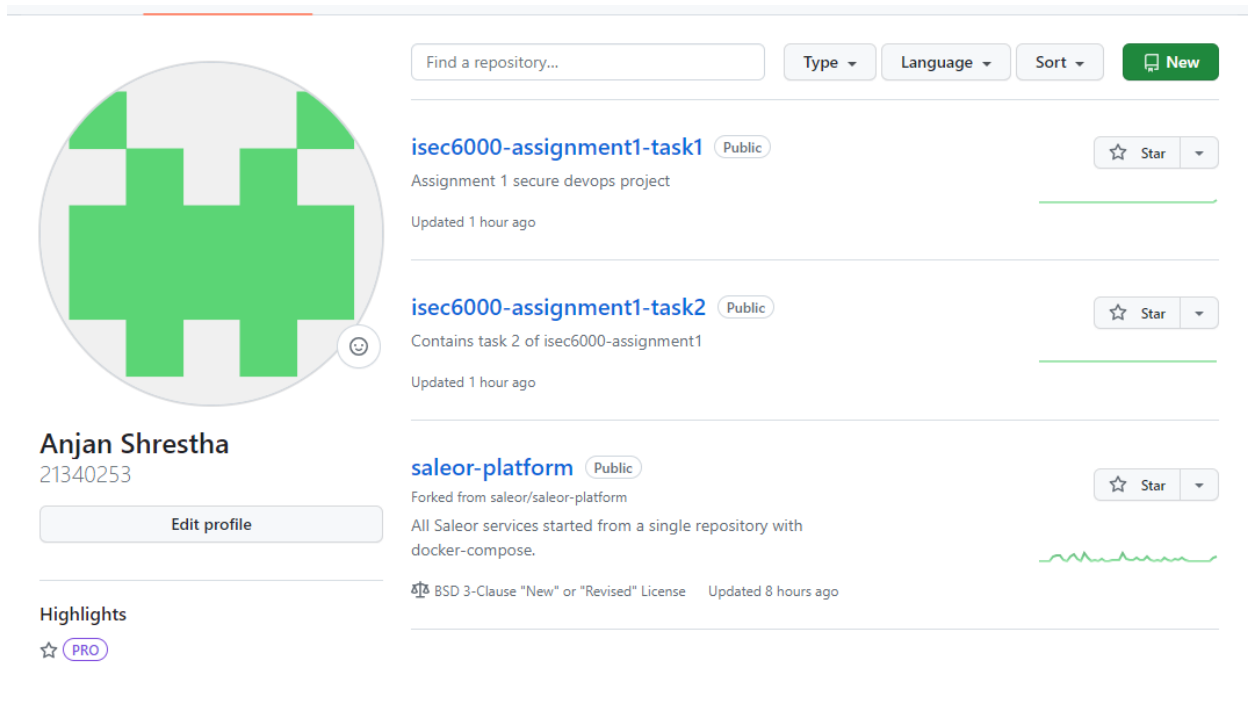
Kubernetes clusters

Status	Name	Location	Mode	Number of nodes	Total vCPUs	Total memory	Notifications
✓	autopilot-cluster-1	us-central1	Autopilot	0	0	0 GB	

Below the table, a terminal window is open, showing the following text:

```
Welcome to Cloud Shell! Type "help" to get started.
Your Cloud Platform project in this session is set to assignment1-398415.
Use "gcloud config set project [PROJECT_ID]" to change to a different project.
strangersth@cloudshell:~ (assignment1-398415)$
```

3. Github public repository created.



Find a repository... Type Language Sort New

Anjan Shrestha
21340253

Edit profile

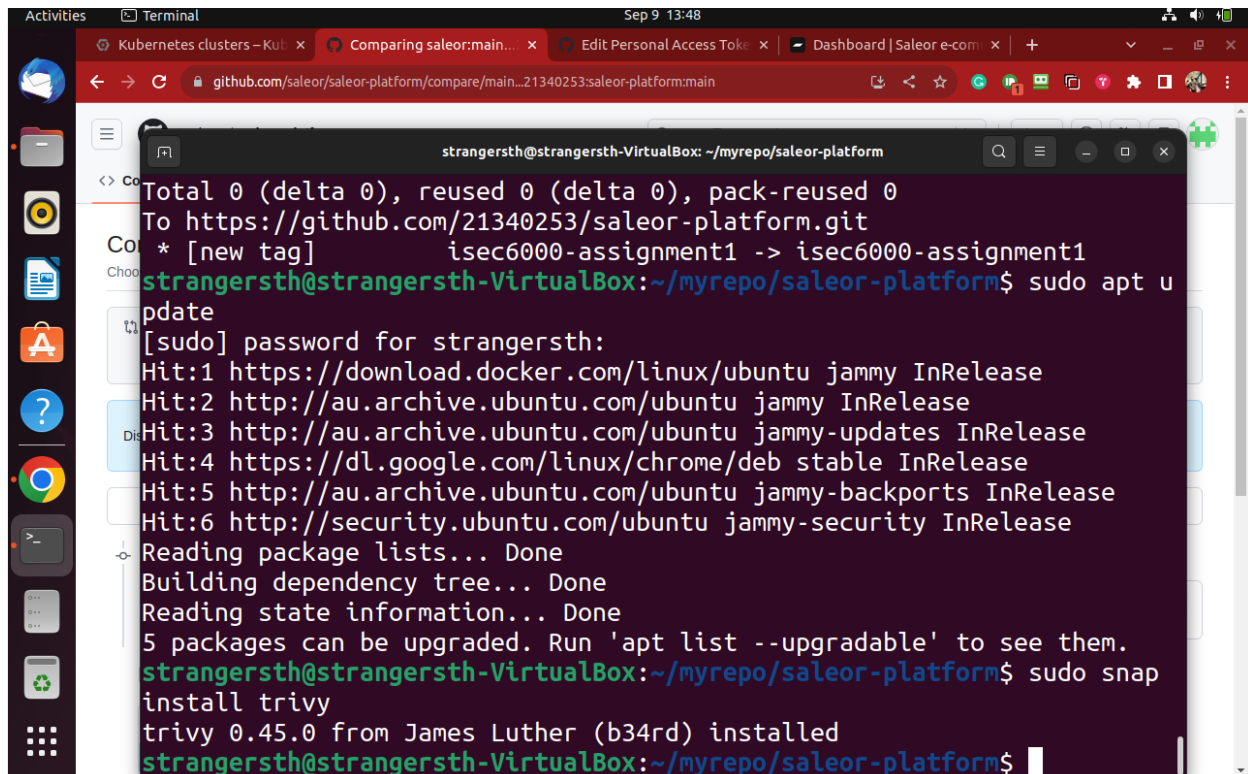
Highlights
☆ PRO

isec6000-assignment1-task1 Public
Assignment 1 secure devops project
Updated 1 hour ago

isec6000-assignment1-task2 Public
Contains task 2 of isec6000-assignment1
Updated 1 hour ago

saleor-platform Public
Forked from saleor/saleor-platform
All Saleor services started from a single repository with docker-compose.
BSD 3-Clause "New" or "Revised" License Updated 8 hours ago

4. Installed Trivy



```
strangersth@strangersth-VirtualBox: ~/myrepo/saleor-platform
Total 0 (delta 0), reused 0 (delta 0), pack-reused 0
To https://github.com/21340253/saleor-platform.git
* [new tag]          isec6000-assignment1 -> isec6000-assignment1
strangersth@strangersth-VirtualBox:~/myrepo/saleor-platform$ sudo apt u
update
[sudo] password for strangersth:
Hit:1 https://download.docker.com/linux/ubuntu jammy InRelease
Hit:2 http://au.archive.ubuntu.com/ubuntu jammy InRelease
Hit:3 http://au.archive.ubuntu.com/ubuntu jammy-updates InRelease
Hit:4 https://dl.google.com/linux/chrome/deb stable InRelease
Hit:5 http://au.archive.ubuntu.com/ubuntu jammy-backports InRelease
Hit:6 http://security.ubuntu.com/ubuntu jammy-security InRelease
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
5 packages can be upgraded. Run 'apt list --upgradable' to see them.
strangersth@strangersth-VirtualBox:~/myrepo/saleor-platform$ sudo snap
install trivy
trivy 0.45.0 from James Luther (b34rd) installed
strangersth@strangersth-VirtualBox:~/myrepo/saleor-platform$
```

5. Implementation of container image vulnerability scanning using trivy tool for ensuring secure configuration of containers

```
strangersth@strangersth-VirtualBox: ~/myrepo/saleor-platform$ trivy image ghcr.io/saleor/saleor:3.15.4
2023-09-09T13:49:56.623+0800 INFO Need to update DB
2023-09-09T13:49:56.623+0800 INFO DB Repository: ghcr.io/aquasecurity/trivy-db
2023-09-09T13:49:56.623+0800 INFO Downloading DB...
39.51 MiB / 39.51 MiB [-----] 100.00% 4.18 MiB p/s 9.7s
2023-09-09T13:50:07.816+0800 INFO Vulnerability scanning is enabled
2023-09-09T13:50:07.822+0800 INFO Secret scanning is enabled
2023-09-09T13:50:07.822+0800 INFO If your scanning is slow, please try '-scanners vuln' to disable secret scanning
2023-09-09T13:50:07.822+0800 INFO Please see also https://aquasecurity.github.io/trivy/v0.45/docs/scanner/secret/#recommendation for faster secret detection
2023-09-09T13:50:51.578+0800 INFO Detected OS: debian
2023-09-09T13:50:51.579+0800 INFO Detecting Debian vulnerabilities...
2023-09-09T13:50:51.651+0800 INFO Number of language-specific files: 2
2023-09-09T13:50:51.651+0800 INFO Detecting python-pkg vulnerabilities...
```

Activities Terminal Sep 9 13:51 strangersth@strangersth-VirtualBox: ~/myrepo/saleor-platform

ghcr.io/saleor/saleor:3.15.4 (debian 12.1)

Total: 137 (UNKNOWN: 0, LOW: 105, MEDIUM: 23, HIGH: 9, CRITICAL: 0)

Library	Vulnerability	Severity	Status	Installed
Version	Fixed Version		Title	
apt	CVE-2011-3374	LOW	affected	2.6.1
not	It was found that apt-key in apt, all versions, d			
	correctly...			
	https://avd.aquasec.com/nvd/cve-2011-3374			

Activities Terminal Sep 9 13:52 strangersth@strangersth-VirtualBox: ~/myrepo/saleor-platform

bsdutils	CVE-2022-0563	1:2.38.1-5+b
chsh when	partial disclosure of arbitrary files in chfn and	
	compiled with...	
	https://avd.aquasec.com/nvd/cve-2022-0563	
coreutils	CVE-2016-2781	will_not_fix 9.1-1
the parent	coreutils: Non-privileged session can escape to t	
	session in chroot	
	https://avd.aquasec.com/nvd/cve-2016-2781	

Activities Terminal Sep 9 13:52 strangersth@strangersth-VirtualBox: ~/myrepo/saleor-platform

	CVE-2017-18018	affected
and chgrp	coreutils: race condition vulnerability in chown	
	https://avd.aquasec.com/nvd/cve-2017-18018	
gcc-12-base	CVE-2022-27943	12.2.0-14
stack	libiberty/rust-demangle.c in GNU GCC 11.2 allows	
	exhaustion in demangle_const	
	https://avd.aquasec.com/nvd/cve-2022-27943	

