

## **Configuration Manual**

MSc Industrial Internship Cyber Security

Rohit Anand Ahuja Student ID: x21168296

School of Computing National College of Ireland

Supervisor: Vikas Sahni

### National College of Ireland



#### **MSc Project Submission Sheet**

	School of Computing		
	Rohit Anand Ahuja		
Student Name:			
	21168296		
Student ID:			
	MSc in Cybersecurity		2022-2023
Programme:		Year:	
	MSc Industrial Internship		
Module:			
	Vikas Sahni		
Lecturer:			
Submission	06/01/2023		
Due Date:			
	Securing the End Points of Microservices using	g GitLa	b Client-Based
<b>Project Title:</b>	Authentication.		
-			
	2136		
Word Count:	Page Count: 28		
	-		

I hereby certify that the information contained in this (my submission) is information pertaining to research I conducted for this project. All information other than my own contribution will be fully referenced and listed in the relevant bibliography section at the rear of the project.

<u>ALL</u> internet material must be referenced in the bibliography section. Students are required to use the Referencing Standard specified in the report template. To use other author's written or electronic work is illegal (plagiarism) and may result in disciplinary action.

	ROHIT ANAND AHUJA
Signature:	
	06/01/2023
Date:	

#### PLEASE READ THE FOLLOWING INSTRUCTIONS AND CHECKLIST

Attach a completed copy of this sheet to each project (including multiple copies)	
Attach a Moodle submission receipt of the online project submission, to each project (including multiple copies).	
You must ensure that you retain a HARD COPY of the project, both	
for your own reference and in case a project is lost or mislaid. It is not sufficient to keep a copy on computer.	

Assignments that are submitted to the Programme Coordinator Office must be placed into the assignment box located outside the office.

Office Use Only	
Signature:	
Date:	
Penalty Applied (if applicable):	

## **Configuration Manual**

Rohit Anand Ahuja Student ID: 21168296

## 1 Deploying a Kubernetes Cluster on AWS EKS (Elastic Kubernetes Service)

Here are the steps to deploy a Kubernetes cluster on AWS EKS with screenshots:

1. Sign in to the AWS Management Console and open the Amazon EKS console at <u>https://console.aws.amazon.com/eks/</u> and click on create cluster button.

aws Services Q Search	[Alt+S]	区 👃  Ohio 🕶 Rohit 🕶
Amazon Elastic × Kubernetes Service	EKS > Clusters	٥
Clusters New	New Kubernetes versions are available for 1 cluster.	×
<ul> <li>Related services</li> <li>Amazon ECR</li> <li>Container storage for EKS</li> </ul>	Clusters (1) Info	C Delete Add cluster ▲
AWS Batch Batch computing on EKS	Q. Filter cluster by name, status, kubernetes version, or provider Cluster name Status V Kubernetes version	
Documentation 🛂 Submit feedback	○ spot2azuseast2	EKS
Feedback Looking for language selection?	ind it in the new Unified Settings [2]	© 2023, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

Figure 1: AWS EKS Create Cluster Page

2. On the "Create Cluster" page, enter a name for the cluster and select the desired service role. Then, choose a Kubernetes version and click the "Next" button. Kubernetes v1.21 has been selected for the proposed research.

Configure cluster	Configure cluster
Step 2 Specify networking	Cluster configuration Info
Step 3 Configure logging	Name Enter a unique name for this cluster. This property cannot be changed after the cluster is created.
Step 4 Select add-ons	The cluster name should begin with letter or digit and can have any of the following characters: the set of Unicode letters, digits, hyphens and underscores. Maximum length of 100.
Step 5 Configure selected add-ons settings	Kubernetes version     Info       Select the Kubernetes version for this cluster.       1.21
Step 6 Review and create	Cluster service role Info Select the IAM role to allow the Kubernetes control plane to manage AWS resources on your behalf. This property cannot is changed after the cluster is created. To create a new role, follow the instructions in the Amazon EKS User Guide 2. eks-quickstart-ControlPlane  C
	Secrets encryption Info Once turned on, secrets encryption cannot be modified or removed.
	Turn on envelope encryption of Kubernetes secrets using KMS Envelope encryption provides an additional layer of encryption for your Kubernetes secrets.
	Tags (0) Info
	This cluster does not have any tags.           Add tag           Remaining tags available to add: 50

Figure 2: Configure Cluster Page

3. On the "Configure Cluster" page, choose the VPC, subnets, and security group for the cluster. Configure the Kubernetes API server endpoint access as Private. Click the "Next" button.

aws	Services Q Search	[Alt+S]
≡	Step 1 Configure cluster	Specify networking
	Step 2 Specify networking	Networking Info These properties cannot be changed after the cluster is created.
	Step 3 Configure logging Step 4 Select add-ons Step 5 Configure selected add-ons settings Step 6 Review and create	VPC info   Beter a vert to use for your EKS cluster resources.To create a new VPC, go to the VPC console.   Vpc-08e89db9107b0c9b010efault   C   Submets info Bose the subnets in your VPC where the control plane may place elastic network interfaces (ENIs) to facilitate communication with your cluster. To create a new subnet, go to the corresponding page in the VPC console. Submet-04cbbdacc17721f19 x submet-018a85d45bc035684 x Submet-029b80a7db3a677c0 x Submet-029b80a7db3a677c0 x Submet-029b80a7db3a677c0 x Security groups info Consecuter IP address family info Consecuter IP address family info Consecuter IP address family info Configure Kubernetes service IP address range info Configure Kubernetes service IP address range info Suprime Configure Kubernetes service IP address range info Configure Kubernetes service IP address range info Configure Kubernetes service IP address range info Suprime Configure Kubernetes service IP address range info
		Cluster endpoint access Info         Configure access to the Kubernetes API server endpoint.         Public         The cluster endpoint is accessible from outside of your VPC. Worker node traffic will leave your VPC to connect to the endpoint.         Public and private         The cluster endpoint is accessible from outside of your VPC. Worker node traffic to the endpoint will stay within your VPC.         Private         The cluster endpoint is only accessible through your VPC. Worker node traffic to the endpoint will stay within your VPC.         Cancel       Previous

Figure 3: Specify Networking Page

4. Skip Step 3,4,5 of AWS EKS Cluster Creation and at the last step 6 i.e., Review and Create – Click on Create.

aws	Services	Q Search		[Alt+S]			
=			Control plane logging				
			API server off	Audit off		Authenticator off	
			Controller manager off	Scheduler off			
			Step 4: Add-ons				Edit
			Selected add-ons				
			Q, Find add-on				< 1 >
			Add-on name	Туре	▼ Status	5	
			coredns	networking	⊘ Ins	talled by default	
			kube-proxy	networking	⊘ Ins	talled by default	
			vpc-cni	networking	⊘ Ins	talled by default	
			Step 5: Versions				Edit
			Selected add-ons version				
			Add-on name		Version		
			kube-proxy		v1.21.2-eksbuild	.2	
			Add-on name coredns		Version v1.8.4-eksbuild.1	1	
			Add-on name vpc-cni		Version v1.10.1-eksbuild	.1	
						Cancel Previous	Create

Figure 4: Create and Review Cluster Page

- 5. This step deploys the Kubernetes cluster on AWS EKS; cluster will be created in 10-15 mins along with one EKS Bastion Host for managing Kubernetes cluster.
- 6. Once the cluster is created, go to the compute tab of the created cluster and click on add node group to add worker nodes.

aws iii Services Q Search	[Alt+S]	<b>D</b> 4	Ohio 🔻	Rohit •
Amazon Elastic × Kubernetes Service	▼ Cluster info Info			0
Clusters New	Kubernetes version Info Status Provider 1.21 OActive EKS			
Related services     Amazon ECR     Container storage for EKS	Overview Resources Compute Networking Add-ons Authentication Logging Update history	Tags		
AWS Batch Batch computing on EKS	Nodes (2) Info			
Documentation 🖸	Q Filter Nodes by property or value		< 1 >	
Submit feedback	Node name         Instance type         V         Node group         V         Created		▼ Status ⊽	
	ip-10-0-18-56.us-east-2.compute.internal t3.medium - Greated ☐ December 23, 2022, 19:00 (UT	FC+00:00)	⊘ Ready	
	ip-10-0-32-251.us-east-2.compute.internal 13.medium - Created	TC+00:00)	⊘ Ready	
	Node groups (0) Info	lete 🚺	Add node group	]
	Group name 🔺 Desired size 🔻 AMI release version 🔻 Launch template	$\nabla$	Status v	
	No node groups			

**Figure 5: Compute tab of Cluster** 

7. On the configure node page, write the node name and specify the IAM role and click on next.

Step 1 Configure node group Step 2	<b>Configure node group</b> Info A node group is a group of EC2 instances that supply compute capacity to your Amazon EKS cluster. You can add mult node groups to your cluster.
Set compute and scaling configuration 	Node group configuration These properties cannot be changed after the node group is created.
Specify networking	Name Assign a unique name for this node group.
Step 4 Review and create	node1         The node group name should begin with letter or digit and can have any of the following characters: the set of Unicode letters, digits, hyphens and underscores. Maximum length of 63.         Node IAM role       Info         Select the IAM role that will be used by the nodes. To create a new role, go to the IAM console.
	eks-quickstart-ManagedNodeInstance <ul> <li>C</li> <li>The selected role must not be used by a self-managed node group as this could lead to a service interruption upon managed node group deletion.</li> </ul>
	Learn more 🔀

8. On the "Add Worker Nodes" page, specify the Amazon EC2 instances that will be used as worker nodes for the cluster. Choose the instance type, auto scaling group configuration, and other options. When done, click the "Next" button.

WS Services Q Search	[Alt+S]
EKS > Clusters > spot2azuseast	2 > Add node group
Step 1 Configure node group	Set compute and scaling configuration
Step 2 Set compute and scaling	Node group compute configuration These properties cannot be changed after the node group is created.
Configuration Step 3	AMI type Info Select the DIS-optimized Amazon Machine Image for nodes.
Specify networking	Amazon Linux 2 (AL2_x86_64)
Step 4 Review and create	Capacity type Select the capacity purchase option for this node group.
	On-Demand 🔻
	Instance types Info Select instance types you prefer for this node group.
	Select
	t3.medium X vCPU: 2.vCPUs Memory: 4 GiB Network: Up to 5 Gigabit Max ENt: 3 Max IPs: 18
	Disk size
	20 GIB
	Node group scaling configuration
	Desired size Set the desired number of nodes that the group should launch with initially.           2         nodes
	Minimum size Set the minimum number of nodes that the group can scale in to.
	2 nodes
	Maximum size Set the maximum number of nodes that the group can scale out to.
	2
	Node group update configuration Info
	Maximum unavailable Set the maximum number or percentage of unavailable nodes to be tolerated during the node group version update.
	Number     Enter a number     Specify a percentage
	Value           1         node
	Cancel Previous Next

Figure 7: Node Configuration Page

9. Click on create on the last page of the node group configuration.

Desired size	Minimum size	Maximum size	
2 nodes	2 nodes	2 nodes	
Node group update config	juration		
Maximum unavailable			
1 node			
ep 3: Networking			Edit
ep 3: Networking Node group network conf	iguration		Edit
ep 3: Networking Node group network conf	iguration Configure SSH access to nodes		Edit
P 3: Networking Node group network conf Subnets subnet-00c19e57983207c90	iguration Configure SSH access to nodes off		Edit
P 3: Networking Node group network conf Subnets subnet-00c19e57983207c90 subnet-04dfb4c94a8d05c19 subnet-04dfb4c94a8d05c19	iguration Configure SSH access to nodes off		Edit

Figure 8: Create Node Group

10. Once the cluster is ready, the cluster can be viewed under EKS Bastion Host, by firing the below command as shown in the screenshots:

sh-1.25 kubectl get suc							
SII 4.20 Kube	CUI YEL DVC						
NAME	TYPE	CLUSTER-IP	EXTERI	NAL-IP	PORT (S)	AGE	
kubernetes	ClusterIP	172.20.0.1	<none:< td=""><td>&gt;</td><td>443/TCP</td><td>19d</td><td></td></none:<>	>	443/TCP	19d	
sh-4.2\$ kube	ctl get node:	s -A					
NAME				STATUS	ROLES	AGE	VERSION
ip-10-0-18-56.us-east-2.compute.internal				Ready	<none></none>	10d	v1.21.14-eks-fb459a0
ip-10-0-32-251.us-east-2.compute.internal			Ready	<none></none>	19d	v1.21.14-eks-fb459a0	
sh-4.2\$							



## 2 Create Cluster Management Project on Gitlab

Follow these steps:

- 1. Create a group in GitLab.
- 2. Click on the "New project" or "New repository" button.
- 3. Click on the "Import" button.
- 4. Select the "From a template" option.
- 5. Select the "GitLab Cluster Management" template and click "Import".
- 6. Enter "Cluster Management" as the project name.

7. Click the "Create project" button.

After completing these steps, a new project in GitLab that is based on the GitLab Cluster Management template will be created. Use this project to manage to deploy GitLab agent and applications to a Kubernetes cluster.

$\downarrow$ $\equiv$ Q Search GitLab			• · · · · · · · · •
C Cluster Management	dassgroup > Cluster Management		
🤞 Ultimate Trial 🛛 Day 20/30	-		
Project information	Profile was successfully updated		×
Repository	Cluster Managemen		
Issues 0	Project ID: 41867367 👸 Leave p	project	ביא Star 0 ע Fork 0 מ
3 Merge requests 0	- 5 Commits 😵 1 Branch 🖉 0 Tags 🗔	824 KB Project Storage	
2 CI/CD			
D Security & Compliance	Adding Manfest Security Scanning		(文) 77bb355c 昂
Deployments	Rohit Ahuja authored 2 weeks ago		
Packages and registries			
Infrastructure	master v cluster-management / +	Y Find file	Web IDE V Clone V
Monitor	문 README 한 MIT License 문 CON	TRIBUTING 🖹 CI/CD configuration 🕀 Add CHANGELOG	
Analytics	Configure Integrations		
🛛 Wiki			
🕻 Snippets	Name	Last commit	Last update
Settings	🗅 .gitlab/agents/spot2azuseast2-a	Adding Manfest Security Scanning	2 weeks ago
	applications	Update helmfile.yaml, applications/cert-man	2 weeks ago
Collapse sidebar	landi di secol	Initialized from 1018 als Cluster Management	3 months and

Figure 10: Cluster Management Gitlab Project

## **3** Register the Gitlab Agent for Kubernetes.

Connect to the EKS Bastion Host, which was deployed earlier, and fire the below commands to register the GitLab agent.



Figure 11:Gitlab Agent Setup

Config token can be acquired by following the steps in: https://docs.gitlab.com/ee/user/clusters/agent/install/

Once the agent has been installed, the agent will reflect in GitLab Kubernetes cluster and also on AWS EKS under Cluster Management Project as shown below:



Figure 12:Gitlab Agent in Gitlab Kubernetes Cluster

sh-4.2\$ kubectl get pods -A   grep "spot?	2azuseast2-agent1"			
gitlab-agent-spot2azuseast2-agent1	scan-vulnerabilityreport-54d958d484-kxjrv	0/1	Completed	10d
gitlab-agent-spot2azuseast2-agent1	scan-vulnerabilityreport-55cbd67ff7-j4prp	0/1	Completed	10d
gitlab-agent-spot2azuseast2-agent1	<pre>scan-vulnerabilityreport-6458d55fb8-8kfg2</pre>	0/1	Completed	10d
gitlab-agent-spot2azuseast2-agent1	scan-vulnerabilityreport-6677f5d548-qdskl	0/1	Completed	10d
gitlab-agent-spot2azuseast2-agent1	scan-vulnerabilityreport-674b77f559-fxlnk	0/1	Completed	10d
gitlab-agent-spot2azuseast2-agent1	scan-vulnerabilityreport-786b77889f-2rpbx	0/1	Completed	14d
gitlab-agent-spot2azuseast2-agent1	<pre>scan-vulnerabilityreport-797b76d9cb-6rkcf</pre>	0/1	Completed	10d
gitlab-agent-spot2azuseast2-agent1	scan-vulnerabilityreport-7b4bd8c44-9cffj	0/1	Completed	10d
gitlab-agent-spot2azuseast2-agent1	scan-vulnerabilityreport-7fc557c567-4ndd8	0/1	Completed	10d
gitlab-agent-spot2azuseast2-agent1	<pre>scan-vulnerabilityreport-845cf48f7d-c9n15</pre>	0/1	Completed	14d
gitlab-agent-spot2azuseast2-agent1	spot2azuseast2-agent1-git1ab-agent-bb86cff8c-1bk17	1/1	Running	10d
sh-4.2\$				

Figure 13: Gitlab Agent deployed in Kubernetes Cluster

## 4 Deploy Isolated Application Build and Application Environment Projects.

Application Build and Application Environment can be deployed using the below steps:

- 1. Log in to GitLab account.
- 2. Click the "Import project" button in the top-right corner of the dashboard.
- 3. Enter the URL of the Git repository that want to import, and click the "Create project" button.
- 4. GitLab will then import the project and create a new repository for it in the registered account.
- 5. Once the import is complete, GitLab will redirect to the project page for the newly-imported repository.

Application Build URL: https://gitlab.com/classgroup6/rohit\_ahuja/hello-world.git

Application Environment URL: <u>https://gitlab.com/classgroup6/rohit\_ahuja/world-greetings-env-1.git</u>

🤟 🔳 🔍 Search GitLab	)	Z		• · D n · · · · · · · · · · · · · · · · ·
H Hello World		classgroup > rohit_ahuja > Hello World		
↓     Ultimate Trial     Day 2       ↓     Project information       ▶     Repository       ▶     Issues	0	Hello World (*) Project ID: 41893685 (*) - 197 Commits (*) 1 Branch (?) 3	Tags 🛛 🖬 11.7 MB Project Storage	□ ~ ☆ Star 0
<ul> <li>Merge requests</li> <li>CI/CD</li> </ul>	0	Update microwebserver.py Rohit Ahuja authored 5 hours	ado	✓ 18d28c5a B
<ul> <li>Security &amp; Compliance</li> <li>Deployments</li> <li>Packages and registries</li> </ul>		main v hello-world / + v	F	ind file Web IDE 🔹 Clone 🗸
<ul> <li>Infrastructure</li> <li>Monitor</li> <li>Acceletion</li> </ul>		README     Configure Integrations	an Add LICENSE Add CHANGELOG Add CO	NTRIBUTING 🛛 🗄 Add Kubernetes cluster
Wiki		Name	Last commit	Last update
X Snippets		.gitlab/ci_includes	Update .gitlab/ci_includes/increment_semve	8 months ago
Ø Settings		🗅 src	Update microwebserver.py	5 hours ago
Collapse sidebar		Jitlab-ci.yml	Update .gitlab-ci.yml file	2 weeks ago

**Figure 14: Application Build** 

븢 😑 🔍 Search GitLab			□ · D 11 · G @•
A Application Environment	classgroup > rohit_ahuja > Application Enviro	nment	
Ultimate Trial Day 20/30  Project information Repository Usues 0	A Application Enviro Project ID: 41894701 &	Donment⊕ Tags 🖶 <b>3.8 MB</b> Project Storage	□ ~ ☆ Star 0 ♥ Fork 0
Werge requests   0     Ø   CI/CD	production: 1.0.38 (Deployed d Rohit Ahuja authored 5 hours a	ue to being found in version tag of latest-prod image) go	(≫) 98c0132e ↑ ↑ ↑ ↑ ↑ ↑ ↑ ↑ ↑ ↑
<ul><li>Security &amp; Compliance</li><li>Deployments</li></ul>	main v world-greetings-env-1 /	+ ~	ind file Web IDE 🔹 Clone 🗸
Packages and registries for Infrastructure	README     CI/CD configuration     Configure Integrations	Add LICENSE Add CHANGELOG	NTRIBUTING
Analytics	Name	Last commit	Last update
Q Wiki	🛅 .gitlab	Update .gitlab-ci.yml, update-manifests.gitla	8 months ago
Solution     Settings	🗅 manifests	production: 1.0.38 (Deployed due to being f	5 hours ago
•	🗅 packages	Update 2 files	2 weeks ago
Collapse sidebar	🤟 .gitlab-ci.yml	Update .gitlab-ci.yml	2 weeks ago

**Figure 15: Application Environment** 

# 5 Running the Application Build and Saving the Container Image

To create a deploy token for a container registry in GitLab:

- 1. Start a pipeline run for the project that i.e., Application Build. This should create a container image.
- 2. After the pipeline has completed, go to the repository settings for the project.

- 3. In the "Repository" section, click on "Deploy Tokens".
- 4. Click the "Create Deploy Token" button.
- 5. Give the token a name, such as "ReadRegistry".
- 6. Under "Scopes", select "read\_registry".
- 7. Click the "Create Deploy Token" button to create the token.

This deploy token can be used to access the container registry for this project.

classgroup > rohit\_ahuja > CI/CD Settings

Q Search page

### Variables

Variables store information, like passwords and secret keys, that you can use in job scripts. Each group can define a maximum of 200 variables. Learn more.

Variables can have several attributes. Learn more.

- Protected: Only exposed to protected branches or protected tags.
- Masked: Hidden in job logs. Must match masking requirements.
- Expanded: Variables with \$ will be treated as the start of a reference to another variable.

Environment variables are configured by your administrator to be protected by default.

Туре	↑ Key	Value	Options	Environments	
Variable	READ_REG_TOKEN	***** [ <mark>°]</mark>	Masked, Expanded	All (default) 🚦	Ø

Figure 16: Read Container Registry Image Token

## 6 Setting up Application Environment Manifests to Monitor Container Image

Steps:

- 1. Edit the manifests of production and staging under the application environment by going under the application environment manifests
- 2. Add the registry link of the application build project under the image tag.



Figure 17: Application Environment Manifests - YAML

## 7 Setting up agent to monitor the changes in Application Environment.

If the agent detects a change to the container image version, it will automatically deploy the updated version to both the staging and production environments. This helps to ensure that the application is always running the most up-to-date version, which can help to improve performance and stability. The agent makes it easy to manage and maintain the application, as it handles the deployment process automatically, freeing up time and resources for other tasks.

In order to instruct the Kubernetes Gitlab Agent to monitor the application environment, will need to edit the config.yaml file. This file is located in the cluster management repository, and can be edited using a text editor or other suitable software. The process of editing the config.yaml file is shown in the accompanying screenshots. To edit the file, simply open using online IDE and make changes. Once the changes have been done, save the file and the agent will begin monitoring the application environment according to the updated configuration. It is important to carefully review and understand the contents of the config.yaml file before making any changes, as incorrect configurations can impact the operation of the agent and the overall performance of the application.





Figure 18: Gitlab Agent Configuration

## 8 Deploying the Application using Pull-Based Approach by Gitlab Agent.

After making any changes to the application build, the application build pipeline will create a registry image and save it in GitLab registry.

classgroup > rohit\_ahuja > Hello World > Repository

#### Edit file

Write	Preview changes						
₿ main	src/microwebse	rver.py	→- No wrap				
1	# From https://g	st.github.com/davidbgk/b10113c3779b8388e96e6d0c44e03a74					
2	import http.serve						
3	import socketserv						
4	from http import	HTTPStatus					
5							
6	class Handler(htt	:p.server.SimpleHTTPRequestHandler):					
7	<pre>def do_GET(se</pre>	elf):					
8	self.send	i_response(HTTPStatus.OK)					
9	self.end	headers ()					
10	self.wfil	e.write(b''' <html></html>					
11	<body sty<="" td=""><td><pre>(le="background:beige"&gt;</pre></td><td></td></body>	<pre>(le="background:beige"&gt;</pre>					
12	<center>&lt;</center>	<pre>img src="https://cdn-icons-png.flaticon.com/512/2345/2345308.png" alt="Research" width="300" height=300"&gt;</pre>					
13	<center></center>	IELLO WORLD					
14	<center></center>	Demo Page for my Research Paper- Simple HTML Page					
15	<center></center>	Config Manual <center></center>					
16	</th <th>(HTML&gt;''')</th> <th></th>	(HTML>''')					
17							
18	httpd = socketser	ver.TCPServer(('', 5000), Handler)					
19	httpd.serve_fore	rer()					
	Commit message	Update microwebserver.py					
	Target Branch main						
Commi	t changes Concel						
Commi	Cancel						

Figure 19: Committing change to Application Build

ⓐrunning         Update microwebserver.py <u>#737361906</u> <sup>®</sup> main → 1d67267e          ⓐ         [atest         ]         [atest         ]	<b>⊘</b>
--	----------

Figure 20: Running the Application Build Pipeline

classgroup > rohit_ahuja > Hello World > Pipe	ines > #737361906	
passed Pipeline #737361906 trigg	gered 1 minute ago by 🌼 Rohit Ah	ıja
Update microwebserver	:ру	
③ 3 jobs for main in 35 seconds (que	ued for 2 seconds)	
P (latest)		
- <b>O-</b> 1d67267e [C		
<b>\$</b> No related merge requests found.		
Pipeline Needs Jobs 3 Tests	0	
.pre	build	.post
etermine-version	kaniko-build	promote-image-to-latest-prod

Figure 21: Updating the latest container image in registry

After the image is stored in the registry, the application environment manifests file will be updated and application will be deployed in the staging and production environment after running the application environment pipeline.

⊘ passed          production: 1.0.3	88 (Deployed due to being found in vers ′ main		$\textcircled{\hspace{0.1cm}} \bullet \textcircled{\hspace{0.1cm}} \bullet \end{array}} \bullet \textcircled{\hspace{0.1cm}} \bullet \textcircled{\hspace{0.1cm}} \bullet \textcircled{\hspace{0.1cm}} \bullet \textcircled{\hspace{0.1cm}} \bullet \textcircled{\hspace{0.1cm}} \bullet \end{array}} \bullet \textcircled{\hspace{0.1cm}} \bullet \textcircled{\hspace{0.1cm}} \bullet \textcircled{\hspace{0.1cm}} \bullet \textcircled{\hspace{0.1cm}} \bullet \textcircled{\hspace{0.1cm}} \bullet \end{array}} \bullet \textcircled{\hspace{0.1cm}} \bullet \textcircled{\hspace{0.1cm}} \bullet \textcircled{\hspace{0.1cm}} \bullet \end{array}} \bullet \textcircled{\hspace{0.1cm}} \bullet \textcircled{\hspace{0.1cm}} \bullet \textcircled{\hspace{0.1cm}} \bullet \end{array}} \bullet \textcircled{\hspace{0.1cm}} \bullet \textcircled{\hspace{0.1cm}} \bullet \end{array} \bullet \\ \bullet \r{\hspace{0.1cm}} \bullet \r{\hspace{0.1cm}} \bullet \r{\hspace{0.1cm}} \bullet \end{array}} \bullet \r{\hspace{0.1cm}} \bullet \hspace{$	<u> </u>
-------------------------------------	---	--	--	----------

Figure 22: Running the Application Environment Pipeline



#### Figure 23: Reading image from the registry

A Application Environment	(queued for main in 26 seconds (queued for	1 second)		
Ultimate Trial Day 20/30	Child pipeline (parent)			
Repository Issues 0	- <b>○</b> 98c0132e Ē			
Merge requests	No related merge requests found.			
Pipelines	Pipeline Needs Jobs 4 Tests 0			
Editor				
Jobs	Upstream	build	update_staging_manifests	update_production_manifests
Schedules	Application Enviro			
Test Cases	< #737365942	Construct-production-manifests	Update-staging-manifests	Update-production-manifests
$\Phi$ Security & Compliance	Parent	construct-staging-manifests		
Deployments				
Packages and registries	L			
lnfrastructure				

Figure 24: Updating the Staging and Production Manifests

The gitlab agent automatically pulls the changes in the application environment manifests and deploy the application to the staging and production environment.





Figure 25:Gitlab Agent pulling changes into the cluster and deploying the application

### Staging Environment:

A Application Environment	classgroup > rohit_ahuja > Application Environment > Environments	
🦊 Ultimate Trial Day 20/30	Available 2 Stopped 0	Enable review app New environment
Project information		
Repository	Q Search by environment name	
D Issues 0	> production	[∄ Open ■ Stop ▮
11 Merge requests 0		
🕼 CI/CD	> staging	[ <sup>7</sup> Open ► × ■ Stop 🚦
$\Phi$ Security & Compliance	· · ···grig	
Deployments		



Figure 26: Application Deployed to Staging

### Production Environment:

🦊 🗮 🔍 Search GitLab			■ × D 11 × G @• + ⊕ ×
A Application Environment	classgroup > rohit_ahuja > Application Environment > Environment	nts	
🦊 Ultimate Trial 🛛 Day 20/30	Available 2 Stopped 0		Enable review app New environment
Project information			
Repository	Q Search by environment name		
D Issues	> production		C Open Stop :
17 Merge requests 0	L		
D Security & Compliance	> staging		C Open 🕨 🗸 🖬 Stop
Deployments			
Environments			
Feature Flags			
Https://wond-gre	eungs-env-1-41894701-production. 5.130.175.09.nlp.io		E ¥ 💀 💆 🔍 🗎 🖉 🛪 🖬 🕥 :
		• ((• ))	
	•	HELLO WORLD	
	Demo I	age for my Research Paper- Simple HTML Page Config Manual	

Figure 27: Application Deployed to Production

## **9** Adding Security Scanning, Kubernetes Manifests Scanning and Container Scanning.

To add security scanning to application by editing the pipeline in Gitlab, the built-in static application security testing (SAST) feature is used. Here are the steps to do this:

- 1. In the Gitlab web interface, navigate to the project containing Application Build
- 2. In the project's "Settings" menu, select "Pipelines" and then click the "Expand" button next to the "Jobs" heading.
- 3. Click the "Edit" button next to the job that builds and test the application. This will open the job's configuration file in the Gitlab code editor.
- 4. To enable SAST add the following:



Figure 28:Adding Security Scanning to Application

5. Save the changes to the configuration file by committing and pushing the changes to the repository.

From now on, Gitlab will automatically run SAST on the application every time the pipeline is triggered. User can view the results of the scan in the "Pipelines" section of the project. If any vulnerabilities are found, Gitlab will provide recommendations on how to fix them.

🦊 ☰ 🔍 Search GitLab					• • •	u.∽ ⊡ ©	• ⊛ -
H Hello World	Vulnerability Rep	port			+ s	ubmit vulnerability	1 Export
🦊 Ultimate Trial 🛛 Day 20/30	The Vulnerability Report shows re Learn more.	sults of successful scans o	n your project's default branch, manually a	dded vulnerability records, and v	ulnerabilities found from scar	nning operational en	vironments.
Project information							
Repository	Development vulnerabilities 1	55 Operational vulner	abilities 0				
D Issues 0	Lesturdated Questioners #	727266240					
11 Merge requests 0	Last updated 2 weeks ago #	121200340					
🕼 CI/CD							
D Security & Compliance	Critical	🔶 High	▼ Medium	Low	<ol> <li>Info</li> </ol>	@ U	nknown
Security dashboard	25	29	31	69	0		1
Vulnerability report							
On-demand scans							
Dependency list	Status	Severity	Tool	Activity			
License compliance	iveeds triage + i more	<ul> <li>All sevenues</li> </ul>	* All tools	All activity	•		
Policies	Detected Status	↓ Severity	Description		Identifier	Tool	Activity
Audit events	_						
Configuration	2022-12-19 Needs Triage	<ul> <li>Critical</li> </ul>	CVE-2022-25236 in libexpat1-2.2.10-2 registry.gitlab.com/classgroup6/roh?992674c	ibdce0a9f5caace1479a1d0f6ef908d	CVE-2022-25236	Container Scanning	$\odot$
Deployments							
-	2022-12-19 Needs Triage	<ul> <li>Critical</li> </ul>	CVE-2022-22823 in libexpat1-2.2.10-2 registry.gitlab.com/classgroup6/roh?992674c	ibdce0a9f5caace1479a1d0f6ef908d	CVE-2022-22823	Container Scanning	$\odot$
Collapse sidebar							

Figure 29: Application Security Testing

To add Kubernetes Manifests Scanning :

Edit the update manifests file in the application environment repository and add the below code. This will enable kubernetes manifests scanning for the application.



Figure 30:Adding Kubernetes Manifests Scanning

🔶 😑 🔍 Search GitLab	Z				• • D	11 ~ G ()	•∽ ⊛ -
A Application Environment     Ultimate Trial Day 20/30     Project information	Vulnerability Re Learn more.	port soults of successful scans or	n your project's default branch, manually a	dded vulnerability records, and v	+ Su	ibmit vulnerability ning operational en	t Export ⊥ Export
Repository     Issues	Development vulnerabilities	0perational vulner	abilities 0				
Merge requests   0        Ø CI/CD	Last updated 2 weeks ago	¥727223780					
Security dashboard	Critical	🔶 High	Medium	Low	<ol> <li>Info</li> </ol>	@ U	nknown
Vulnerability report	26	0	110	0	41		0
On-demand scans							
Dependency list License compliance Policies	Status Needs triage +1 more	Severity All severities	✓ All tools	Activity     All activity	~		
Audit events	Detected Status	↓ Severity	Description		Identifier	Tool	Activity
© Deployments - « Collapse sidebar	2022-12-19 Needs Triage	Critical	Roles and ClusterRoles with wildcard RB sive rights to the Kubernetes API and sh e of least privilege recommends to spec ects and actions packages/gitlab-agent/cluster/co ts/c	IAC permissions provide exces ould be avoided. The principl ify only the set of needed obj ilium-install/resources.yaml:11	RBAC Wildcard In Rule	SAST	

Figure 31: Kubernetes Manifests Scanning Report

To add container scanning using Gitlab Agent for Kubernetes:

Edit the following file and add the mentioned lines:

C Cluster Management	master v cluster-management / .gitlab / agents / spot2azuseast2-agent1 / config.yaml						
🦊 Ultimate Trial 🛛 Day 20/30	Adding Manfest Security Scanning						
Project information	Rohit Ahuja authored 2 weeks ago						
Repository							
Files							
Commits	1 #id: = Full group path without instance url 2 # and without leading or trailing slashes.						
Branches	3 # for https://gitlab.com/this/is/an/example, id would be:						
Tags	4 # - id: this/is/an/example 5						
Contributors	6 ci_access:						
Graph	<pre>groups. 8 - id: classgroup6</pre>						
Compare	10 observability:						
Locked Files	11     logging:       12     level: debug						
D Issues	13 14 starboard:						
3 Merge requests	15 cadence: '45 * * * ' #Every hour at 55 minutes past the hour 16						

Figure 32:Adding Container Scanning

Starboard tool developed by aqua security has been used which automatically scans Kubernetes containers.

C Cluster Management	30 Spot2azuseast2-agent1 Created by Rohit Ahuja 2 weeks ago							
Project information  Repository  Issues	> Integration Status Connected							
Merge requests	s 0 Activity Security Access tokens 1							
CI/CD  Security & Compliance	J/CD () Latest scan run against spot2azuseast2-agent1 Vau cap view cap routht for all agents in the Operational Wilegrabilities tablef the wilegrabilities tablef tabl							
Deployments								
Packages and registries	Status		Severity	Image Activity				
lnfrastructure	Needs thage + I fr	lore	Unknown +1	All images				
Kubernetes clusters •	Detected	Status	↓ Severity	Description				
Terraform Google Cloud	2022-12-23	Needs	Low	CVE-2022-0563				
Monitor		Triage		registry.gitlab.com/classgroup6/rohit_ahuja/hello-world/main:7cda07f4dd33f68d30747dddc2c72dbaab5fb32e				
h Analytics	2022-12-23	Needs Triage	low	CVE-2005-2541 registry.gitlab.com/classgroup6/rohit_ahuja/hello-world/main.7cda07f4dd33f68d30747dddc2c72dbaab5fb32e				
📮 Wiki								
X Snippets	2022-12-23	Needs Triage	low 🥚	CVE-2011-4116 registry.gitlab.com/classgroup6/rohit_ahuja/hello-world/main:7cda07f4dd33f68d30747dddc2c72dbaab5fb32e				
<ul> <li>Settings</li> <li>Collapse sidebar</li> </ul>	2022-12-23	Needs Triage	• Low	CVE-2019-19882 registry.gitlab.com/classgroup6/rohit_ahuja/hello-world/main:7cda07f4dd33f68d30747dddc2c72dbaab5fb32e				

Figure 33: Container Scanning Report View

## **10** Scanning Kubernetes Cluster using Kube-Tools

1. Using Kube-Hunter

Kube-Hunter was deployed in one of the Kubernetes pods using the following steps:



Figure 34: Code to install kube-hunter

Session ID: root-0d2f107ba1c5b09f0

Instance ID: i-07d954a1ecaf2542f

sh-4.2\$ kubectl get	pods				
NAME	READY	STATUS	RESTARTS	AGE	
kube-bench-zfnnp	0/1	Completed	0	30h	
kube-hunter-742ql	0/1	Completed	0	31h	
sh-4.2\$					

Figure 35: Kube-hunter in pod

2. Scanning using Kube-Scape

Scanning using Kube-Scape was done by following the below steps:

User need to create an account first on kubescape cloud portal and extract the account id and fire the below commands in kubernetes cluster:



Figure 36: Code to perform Kube-Scape scan

The kubescape will scan the cluster and save the results in the cloud dashboard.

KUBESCAPE =			Rohit Ahuja acco
- CLOUD -	Configuration Scanning		
CLUSTER	Configuration Scanning		
🔛 Dashboard	Search Q		
Config Scanning			
() Image Scanning	arn-aws-eks-us-east-2-03219339 🛐 🧿	arn-aws-eks-us-east-2-90466291 📭 🥑	
🗞 RBAC Visualizer	27 rohit 17 AllC	4 rohit	
CODE			
문 Repository Scanning	2/1 2/1 2/1 2/1	2/1	
Registry Scanning			

Figure 37:Kube Scape Cloud Portal

### References

aquasecurity/kube-hunter: Hunt for security weaknesses in Kubernetes clusters Available at: https://github.com/aquasecurity/kube-hunter (Accessed: 3 January 2023).

Connecting a Kubernetes cluster with GitLab | GitLab (no date). Available at: https://docs.gitlab.com/ee/user/clusters/agent/ (Accessed: 3 January 2023).

Kubescape. Available at: https://cloud.armosec.io/config-scanning (Accessed: 3 January 2023).

Starboard. Available at: https://aquasecurity.github.io/starboard/v0.15.6/ (Accessed: 3 January 2023).

### **Appendix H – Monthly Internship Activity Report**

The Internship Activity Report is a 1-page monthly summary of the activities performed by you and what you have learned during that month. The Internship Activity Report must be signed off by your Company and included in the configuration manual as part of the portfolio submission.

Student Name:	Rohit Anand Ahuja	Student number:	21168296
Company:	RiskSek Private Limited	Month Commencing:	October 2022

- Perform Network and Application Vulnerability Assessments and Penetration Testing activities.
- Involved in other Cyber Security Services offered by the company as required.
- Worked on researching topics and started understanding the working of Kubernetes and its architecture and its literature review.

**Employer comments** 

Student Signature: Rohit Anand Ahuja\_\_\_\_\_Date: 03/01/2023

Industry Supervisor Signature: Sarat Lingamallu\_\_\_\_\_Date: 03/01/2023

### **Appendix H – Monthly Internship Activity Report**

The Internship Activity Report is a 1-page monthly summary of the activities performed by you and what you have learned during that month. The Internship Activity Report must be signed off by your Company and included in the configuration manual as part of the portfolio submission.

Student Name:	Rohit Anand Ahuja	Student number:	21168296
Company:	RiskSek Private Limited	Month Commencing:	November 2022

- Worked on documenting data breaches that commenced in November month.
- Started working on the Design Specification of the proposed research regarding securing the endpoints of the microservices using client-based authentication.
- Worked on learning about AWS EKS services and Gitlab Agent.

**Employer comments** 

Student Signature: Rohit Anand Ahuja\_\_\_\_\_Date: 03/01/2023

Industry Supervisor Signature: Sarat Lingamallu\_\_\_\_\_Date: 03/01/2023

### **Appendix H – Monthly Internship Activity Report**

The Internship Activity Report is a 1-page monthly summary of the activities performed by you and what you have learned during that month. The Internship Activity Report must be signed off by your Company and included in the configuration manual as part of the portfolio submission.

Student Name: F	Rohit Anand Ahuja	Student number:	21168296
Company:	RiskSek Private Limited	Month Commencing:	December 2022

- Worked on documenting data breaches commenced in December month.
- Started working on implementation of integration of AWS EKS and Gitlab. Deployed Kubernetes Cluster on AWS EKS and installed agent in one of the pods.
- Deployed projects and isolated the application build and application environment, added security scanning.
- Evaluated the proposed architecture using tools.

**Employer comments** 

Student Signature: Rohit Anand Ahuja\_\_\_\_\_Date: 03/01/2023

Industry Supervisor Signature: Sarat Lingamallu\_\_\_\_\_Date: 03/01/2023