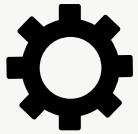


MINISOC



SCOPO DEL PROGETTO



MONITORING

Collezionare, categorizzare e analizzare i dati ricevuti, statistiche ed eventi critici dell'infrastruttura



ANALYSIS

Network analysis, Malware analysis, report di findings



RESPONSE

Fornire capacità di difesa attiva e analisi su tutta l'infrastruttura



SCALABLE & RELIABLE

L'intero progetto è basato su Kubernetes, cloud e soluzioni di autoscaling



MICROSERVIZIO: SOC



- Interagisce con l'utente finale
- Invia richieste agli altri microservizi
- Supporta **l'autenticazione**
- Fornisce le **dashboard** di sicurezza
- **Monitora** le applicazioni scelte dall'utente



MICROSERVIZIO: TOOL



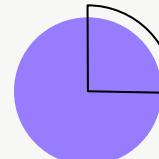
- Utilizza tool come **YARA** e **TSHARK**
- **Network analysis** di *pcap* caricati tramite il SOC
- **Malware analysis** di *file* caricati tramite il SOC
- Raggiungibile solo dal SOC



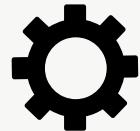
 **VIRUSTOTAL**



 **WIRESHARK**



MICROSERVIZIO: APP



- Semplice servizio **web**
- Applicazione esposta su Internet
- Può essere sostituita con una vera applicazione da monitorare

NEINX



GoAccess





KUBERNETES

Grazie a Kubernetes il deploy può essere automatizzato, esteso e facilmente configurato a runtime. La divisione delle risorse presenti è nel seguente modo

DEPLOYMENT



Microservizi che compongono il progetto

SERVICES



Networking e balancing verso internet

HPA



Autoscale dei microservizi

VOLUMES



Condivisione dei dati tra i Microservizi

CONFIGMAP



Configurazione parametrica





HELM

Helm permette di facilitare il deployment fornendo template personalizzabili.
Abbiamo utilizzato Helm per installare le seguenti risorse

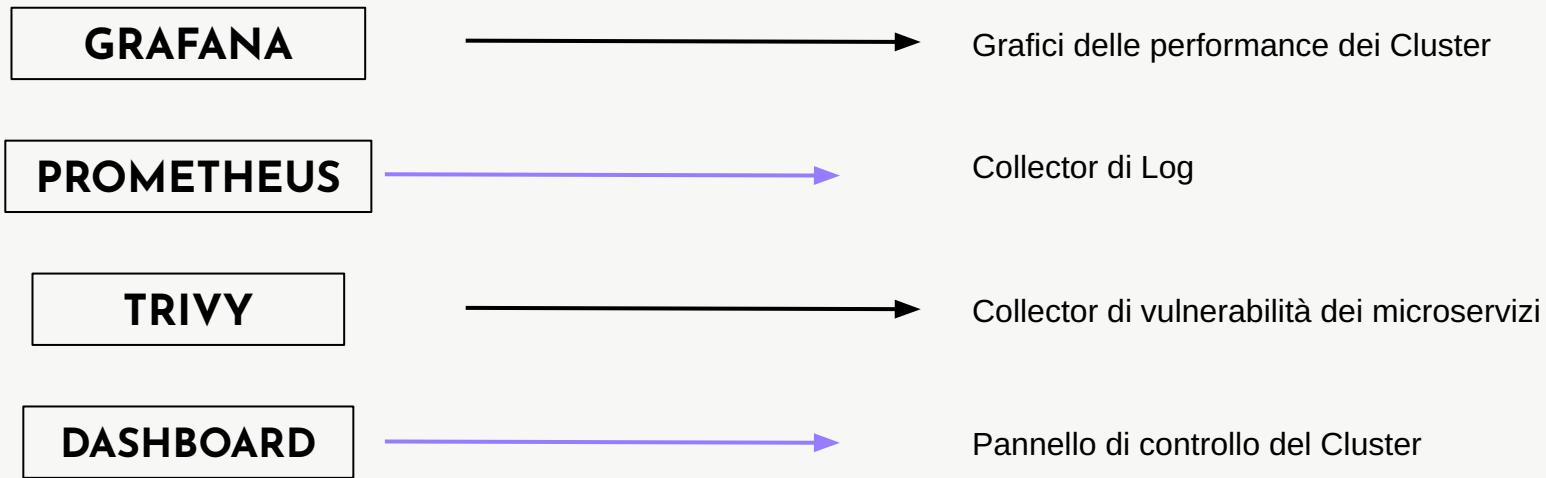
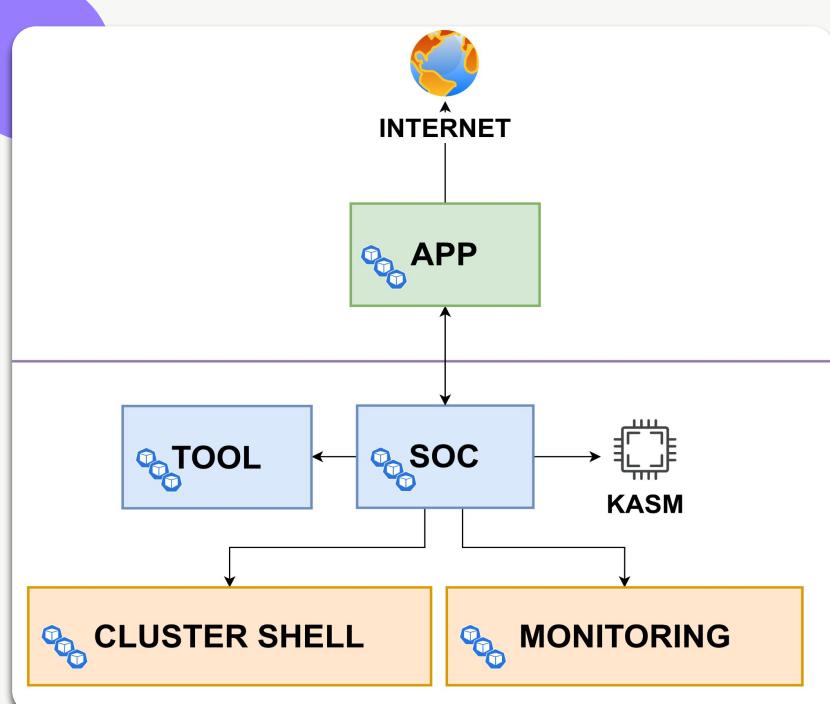
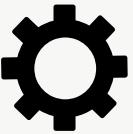


DIAGRAMMA APPLICATIVO





LANDING PAGE

The screenshot shows a dark-themed web application interface. On the left, a sidebar contains navigation links such as Cluster, Security (Network Analyzer, Malware Analyzer, Kasm), Statistics (CoreDNS, Pods Workload - Master, Pods Workload - Worker, Volumes, Networking, Application Statistics), and Trivy. A purple button labeled "MiniSoc" is visible, along with a GitHub link. The main content area features a large, stylized title "MiniSOC" in white and orange. At the bottom of the page, there is footer text: "© FlippaFloppa - Coded by BlessedRebuS, leonardobambini, RootLeo00.", "The GNU General Public License v3.0", and a small "GitHub" logo.



DASHBOARD

Kubernetes All namespaces Search

Workloads > Deployments

CPU Usage

Memory Usage

Deployments

Name	Namespace	Images	Labels	Pods	Created
data-proxy-server	iot	docker.io/umbo-iot/python-data-proxy-server:latest	-	1 / 1	17 hours ago
kubernetes-dashboard-long	kubernetes-dashboard	kong:3.6	app.kubernetes.io/component: app app.kubernetes.io/instance: kubernetes-dashboard app.kubernetes.io/managed-by: Helm app.kubernetes.io/component: metrics-scrapers app.kubernetes.io/instance: kubernetes-dashboard app.kubernetes.io/managed-by: Helm app.kubernetes.io/component: web app.kubernetes.io/instance: kubernetes-dashboard app.kubernetes.io/managed-by: Helm app.kubernetes.io/component: auth app.kubernetes.io/instance: kubernetes-dashboard app.kubernetes.io/managed-by: Helm app.kubernetes.io/component: api app.kubernetes.io/instance: kubernetes-dashboard app.kubernetes.io/managed-by: Helm	1 / 1	4 days ago
kubernetes-dashboard-metrics-scaper	kubernetes-dashboard	docker.io/kubernetes/dashboard-metrics-scaper:1.1.1	app.kubernetes.io/instance: kubernetes-dashboard app.kubernetes.io/managed-by: Helm app.kubernetes.io/component: metrics-scrapers app.kubernetes.io/instance: kubernetes-dashboard app.kubernetes.io/managed-by: Helm	1 / 1	4 days ago
kubernetes-dashboard-web	kubernetes-dashboard	docker.io/kubernetes/dashboard-web:1.3.0	app.kubernetes.io/instance: kubernetes-dashboard app.kubernetes.io/managed-by: Helm app.kubernetes.io/component: web app.kubernetes.io/instance: kubernetes-dashboard app.kubernetes.io/managed-by: Helm app.kubernetes.io/component: auth app.kubernetes.io/instance: kubernetes-dashboard app.kubernetes.io/managed-by: Helm app.kubernetes.io/component: api app.kubernetes.io/instance: kubernetes-dashboard app.kubernetes.io/managed-by: Helm	1 / 1	4 days ago
kubernetes-dashboard-auth	kubernetes-dashboard	docker.io/kubernetes/dashboard-auth:1.1.3	app.kubernetes.io/instance: kubernetes-dashboard app.kubernetes.io/managed-by: Helm app.kubernetes.io/component: auth app.kubernetes.io/instance: kubernetes-dashboard app.kubernetes.io/managed-by: Helm	1 / 1	4 days ago
kubernetes-dashboard-api	kubernetes-dashboard	docker.io/kubernetes/dashboard-api:1.5.0	app.kubernetes.io/instance: kubernetes-dashboard app.kubernetes.io/managed-by: Helm app.kubernetes.io/component: api app.kubernetes.io/instance: kubernetes-dashboard app.kubernetes.io/managed-by: Helm	1 / 1	4 days ago
soc	monitoring	docker.io/library/soc:v1	-	1 / 1	4 days ago
ingress-nginx-controller	ingress-nginx	nginx.ingress.k8s.io/controller:v1.2.0@sha256:db196e0bc1e7254765dec6d3cc0f72a291a091a20c08e770bc50597148	app.kubernetes.io/component: controller app.kubernetes.io/instance: ingress-nginx app.kubernetes.io/name: ingress-nginx app.kubernetes.io/managed-by: Helm	1 / 1	5 days ago
tool	monitoring	docker.io/library/tool:v1	-	1 / 1	8 days ago
emqx-operator-controller-manager	emqx-operator-system	emqx/emqx-operator-controller:2.2.22	app.kubernetes.io/instance: emqx-operator app.kubernetes.io/managed-by: Helm app.kubernetes.io/name: emqx-operator app.kubernetes.io/managed-by: Helm	1 / 1	13 days ago

1 – 10 of 25 | < < > >|



NETWORK ANALYZER

The screenshot displays the Network Analyzer interface within a dark-themed application. On the left, a vertical sidebar menu lists several sections: Dashboard, Security (Network Analyzer, Malware Analyzer, Kasm), Statistics (CoreDNS, Pods Workload - Master, Pods Workload - Worker, Volumes, Networking, Application Statistics, Trivy), and a general Home and Cluster section. The 'Network Analyzer' section is currently selected, indicated by a purple background. The main content area is titled 'Analyzer' and contains a sub-section titled 'Network Analyzer'. Below this are tabs for SSH, HTTP, DNS, ICMP, SSL, and TCP, with 'Network Analyzer' being the active tab. A large dashed rectangular area in the center is labeled 'Drop files here or click to upload.' A 'Clear' button is located just above this area. At the top of the main content area, there is a search bar with the placeholder 'Search here...' and a three-dot menu icon. The top right corner features icons for brightness, notifications, user profile, and settings.



MALWARE ANALYZER

The screenshot displays the Malware Analyzer interface on a dark-themed web application. The left sidebar contains navigation links for Dashboard, Home, Cluster, Security (Network Analyzer, Malware Analyzer), Kasm, Statistics (CoreDNS, Pods Workload - Master, Pods Workload - Worker), Volumes, Networking, Application Statistics, and Trivy. The main content area is titled "Analyzer" and features a "Malware Analyzer" button, a "Clear" button, and a dashed-dotted file upload area with the placeholder text "Drop files here or click to upload." The top right corner includes a search bar, a three-dot menu, and user profile icons.



APPLICATION STATISTICS

Search here...

Last Updated: 2024-05-31 10:52:20 +0000
06/MAY/2024 — 28/MAY/2024

OVERALL ANALYZED REQUESTS

Total Requests 113	Valid Requests 113	Failed Requests 0
Pixel IP Hits 0	Referrals 0	Not Found 5

UNIQUE VISITORS PER DAY - INCLUDING SPIDERS
HTTs HAVING THE SAME IP DATE AND AGENT ARE A UNIQUE VISIT

Date	Hits	Visitors
06/05/2024	~28	~0.8
07/05/2024	~25	~0.7
08/05/2024	~22	~0.6
09/05/2024	~20	~0.5
10/05/2024	~18	~0.4
11/05/2024	~15	~0.3
12/05/2024	~12	~0.2
13/05/2024	~10	~0.1
14/05/2024	~8	~0.1
15/05/2024	~6	~0.1
16/05/2024	~4	~0.1
17/05/2024	~2	~0.1
18/05/2024	~1	~0.1
19/05/2024	~1	~0.1
20/05/2024	~1	~0.1
21/05/2024	~1	~0.1
22/05/2024	~1	~0.1
23/05/2024	~1	~0.1
24/05/2024	~1	~0.1
25/05/2024	~1	~0.1
26/05/2024	~1	~0.1
27/05/2024	~1	~0.1
28/05/2024	~1	~0.1

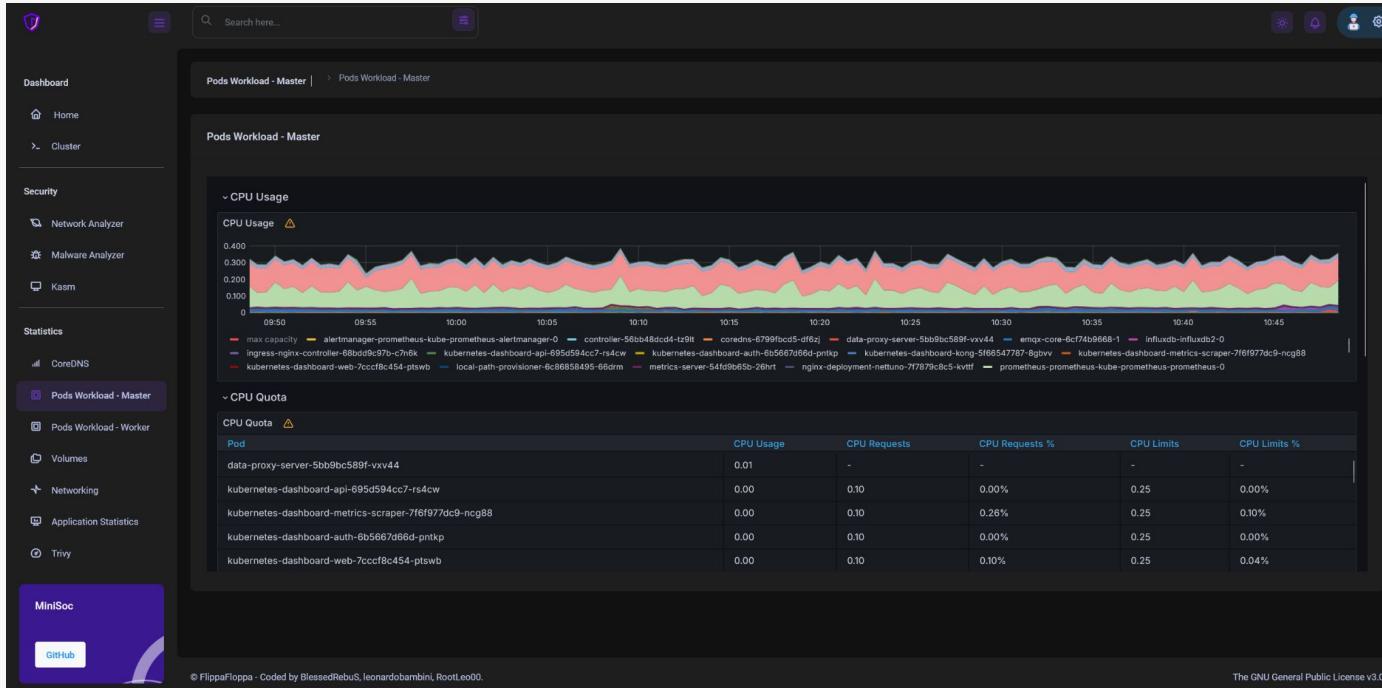
REQUESTED FILES (URLS)
TOP REQUESTS SORTED BY HTTs (AGTS, CUMTS, MAXTS, MTHD, PROT)

File	Hits	Visitors
GET / HTTP/1.1	16	6

The GNU General Public License v3.0



CLUSTER PERFORMANCES



NODI & DEPLOYMENTS



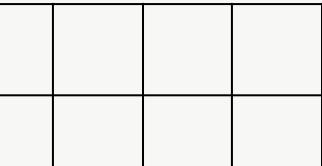
- Ogni elemento dell'applicazione è un **deployment**
- In presenza di poche o nulle richieste ogni deploy ha 1 solo pod
- I deployment sono bilanciati su **due nodi**

Nodes(all) [2]												
NAME↑	STATUS	ROLE	TRAINTS	VERSION	PODS	CPU	MEM	%CPU	%MEM	CPU/A	MEM/A	AGE
k3s-worker	Ready	<none>	0	v1.29.4+k3s1	13	145	2024	3	25	4000	7941	27d
kubernetes	Ready	control-plane,master	0	v1.29.4+k3s1	25	561	4044	7	25	8000	15991	28d

<node>

Deployments(monitored) [7]			
NAME↑	READY	UP-TO-DATE	AVAILABLE AGE
prometheus-grafana	1/1	1	1 24d
prometheus-kube-prometheus-operator	1/1	1	1 24d
prometheus-kube-state-metrics	1/1	1	1 24d
simple-app	1/1	1	1 24d
soc	1/1	1	1 4d4h
tool	1/1	1	1 8d
trivy-operator	1/1	1	1 24d

<deployment>



SERVICES

- I services gestiscono il **networking**
- Divisi in **LoadBalancer** e **ClusterIP**
- External-IP** è legato alla NIC della VM, usando **MetalLB**

```
apiVersion: v1
kind: Service
metadata:
  creationTimestamp: null
  name: soc-svc
  namespace: monitoring
  annotations:
    metallb.universe.tf/allow-shared-ip: "scalable"
spec:
  ports:
    - port: 5000
      protocol: TCP
      targetPort: 5000
  selector:
    app: soc
  sessionAffinity: ClientIP
  sessionAffinityConfig:
    clientIP:
      timeoutSeconds: 10000
  type: LoadBalancer
status:
  loadBalancer: {}
```

Services(monitoring)[12]						
NAME↑	TYPE	CLUSTER-IP	EXTERNAL-IP	PORTS	AGE	
alertmanager-operated	ClusterIP					
prometheus-grafana	LoadBalancer	10.43.196.92	192.168.1.150	http-web:9093>0 tcp-mesh:9094>0 udp-mesh:9094>0/UDP	24d	
prometheus-kube-prometheus-alertmanager	ClusterIP	10.43.26.232		http-web:3000-32323	24d	
prometheus-kube-prometheus-operator	ClusterIP	10.43.61.234		http-web:9093>0 reloader-web:8080>0	24d	
prometheus-kube-prometheus-prometheus	ClusterIP	10.43.142.161		https:443>0	24d	
prometheus-kube-state-metrics	ClusterIP	10.43.22.20		http-web:9090>0 reloader-web:8080>0	24d	
prometheus-operated	ClusterIP			http:8080>0	24d	
prometheus-prometheus-node-exporter	ClusterIP	10.43.90.200		http-web:9090>0	24d	
simple-app	LoadBalancer	10.43.63.40	192.168.1.150	http-metrics:9100>0	24d	
soc-svc	LoadBalancer	10.43.84.210	192.168.1.150	5001>32746	13d	
tool-svc	ClusterIP	10.43.92.154		5000>32529	8d	
trivy-operator	ClusterIP			5001>0	24d	
				metrics:80>0		

<service>



SCALABILITY: HPA



- **Horizontal Pod Autoscaler** impostato su tutti i deployment
- Permette di gestire il carico in maniera **dinamica**
- Ripristina il numero di **pod** una volta passato il picco di carico

Horizontalpodautoscalers (monitoring) [3]						
NAME	REFERENCE	TARGETS	MINPODS	MAXPODS	REPLICAS	AGE
simple-app	Deployment/simple-app	<unknown>/80%	1	100	0	8s
soc	Deployment/soc	8%/80%	1	100	1	13d
tool	Deployment/tool	<unknown>/80%	1	10	1	21s



VOLUME & STORAGE 1/2

- Vengono definiti dei **Persistent Volume** come pool di storage
- Tramite i **Persistent Volume Claim** i pod si legano ai PV
- La capacity dei volumi è definibile a runtime
- Su **AWS** è definito l'**autoscaling** dei volumi



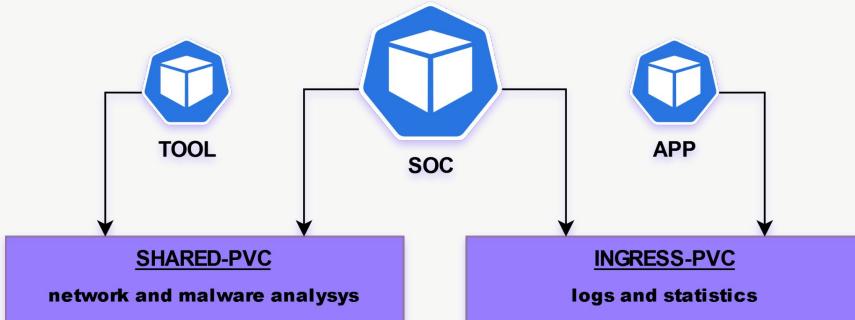
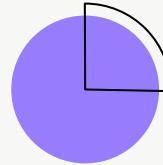
Persistentvolumeclaims (monitoring) [2]						
NAME	STATUS	VOLUME	CAPACITY	ACCESS MODES	STORAGECLASS	AGE
ingress-pvc	Bound	pvc-00634e9f-28af-4954-ac1-1b41448b0016	200Mi	RWO	local-path	25d
shared-pvc	Bound	shared-pv	1Gi	RWO	local-path	15d

NAME	PROVISIONER	RECLAIMPOLICY	VOLUMEBINDINGMODE	ALLOWVOLUMEEXPANSION	AGE
gp2 (default)	kubernetes.io/aws-ebs	Delete	WaitForFirstConsumer	false	82m
gp3 (default)	ebs.csi.aws.com	Retain	WaitForFirstConsumer	true	6m5s

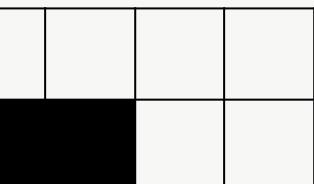
NAMESPACE	NAME	READY	UP-TO-DATE	AVAILABLE	AGE
kube-system	coredns	2/2	2	2	79m
kube-system	ebs-csi-controller	2/2	2	2	77m
monitoring	prometheus-grafana	1/1	1	1	54m
monitoring	prometheus-kube-prometheus-operator	1/1	1	1	54m
monitoring	prometheus-kube-state-metrics	1/1	1	1	54m
monitoring	simple-app	1/1	1	1	40m
monitoring	soc	1/1	1	1	47m
monitoring	tool	1/1	1	1	46m
monitoring	trivy-operator	1/1	1	1	52m
monitoring	volume-autoscaler	1/1	1	1	9s

VOLUME & STORAGE 2/2

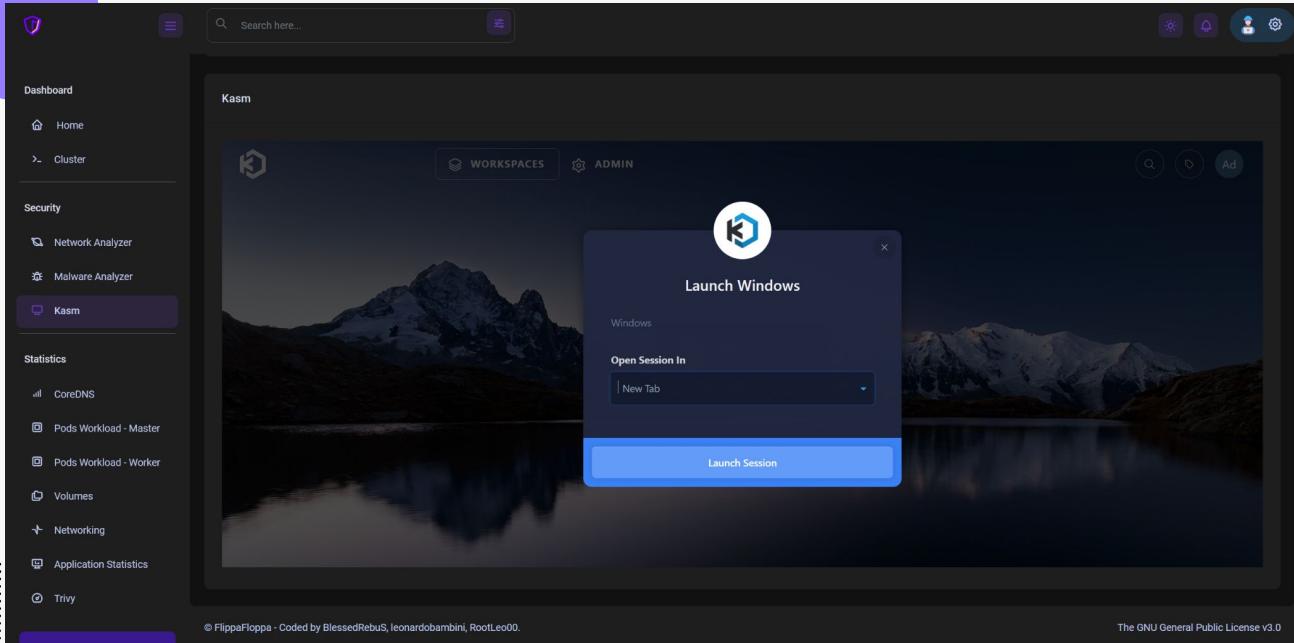
- Il **SOC** fa il mount (centralizza) tutti i volumi
- **Segregazione dei volumi** per questioni di sicurezza
- Richiesta dei dati on demand e non passando via rete



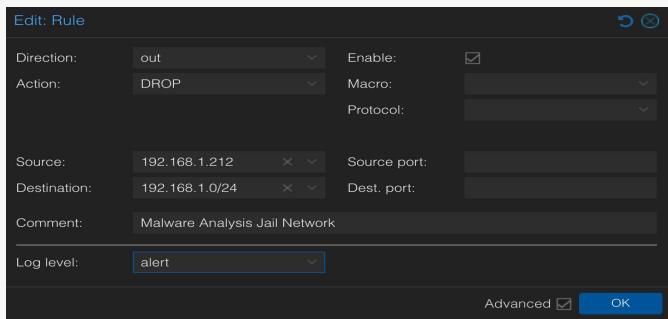
```
containers:
  - image: nginx
    name: nginx
    ...
  - name: goaccess
    command:
      command: [ "/bin/sh", "-c", "--" ]
      args: [ "while true; do goaccess /var/log/nginx/nginx-access.log
-o /var/log/nginx/result.html --log-format=COMBINED; done;" ]
    image: allinurl/goaccess
    imagePullPolicy: Always
  resources:
    requests:
      cpu: 200m
      memory: 32Mi
  terminationMessagePath: /dev/termination-log
  terminationMessagePolicy: File
  volumeMounts:
    - mountPath: /var/log/nginx
      name: nginx-ingress-pvc
```



KASM



The screenshot shows the KASM web interface. On the left, there's a sidebar with navigation links: Dashboard, Home, Cluster, Security (Network Analyzer, Malware Analyzer, Kasm), Statistics (CoreDNS, Pods Workload - Master, Pods Workload - Worker, Volumes, Networking, Application Statistics), and Trivy. The 'Kasm' link is highlighted. The main area has a dark background with a mountain landscape image. A central modal window titled 'Launch Windows' is open, showing a dropdown menu 'Open Session In' with 'New Tab' selected, and a large blue button at the bottom labeled 'Launch Session'.



The dialog box is titled 'Edit: Rule'. It contains the following fields:

Direction:	out	Enable:	<input checked="" type="checkbox"/>
Action:	DROP	Macro:	<input type="text"/>
Protocol:	<input type="text"/>		
Source:	<input type="text"/> 192.168.1.212	Source port:	<input type="text"/>
Destination:	<input type="text"/> 192.168.1.0/24	Dest. port:	<input type="text"/>
Comment:	Malware Analysis Jail Network		
Log level:	<input type="text"/> alert		

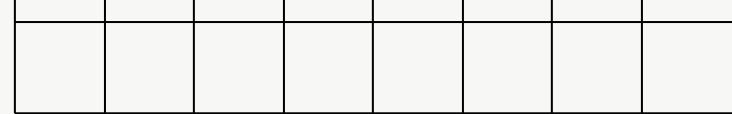
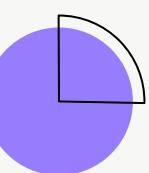
At the bottom right are 'Advanced' and 'OK' buttons.



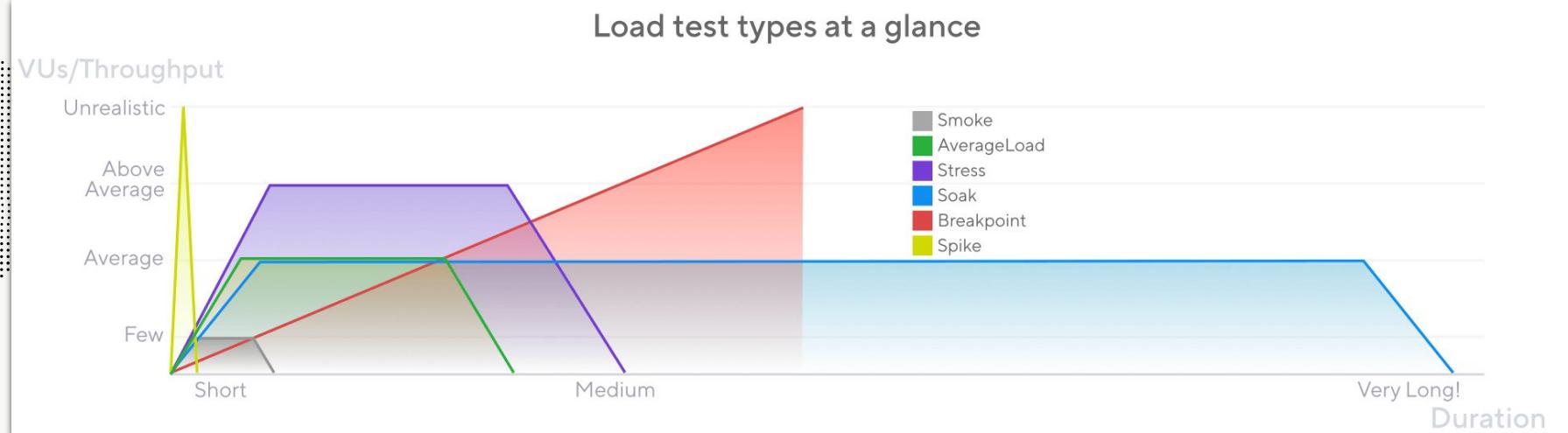
https://soc-svc



https://kasm.soc-svc



BENCHMARKS





SPIKE TEST

```
Context: default
Cluster: default
User: default
K9s Rev: v0.32.4
K8s Rev: v1.29.4+k3s1
CPU: 15%
MEM: 34%
```

```
<0> all
<1> deception
<2> default
```



Horizontalpodautoscalers(all)[1]

NAMESPACE↑	NAME	REFERENCE	TARGETS	MINPODS	MAXPODS	REPLICAS	AGE
monitoring	soc	Deployment/soc	84%/80%	1	100	15	24m

<horizontalpodautoscaler>

```
stages: [
  { duration: '2m', target: 2000 }, // fast ramp-up to a high point
  { duration: '1m', target: 0 }, // quick ramp-down to 0 users
]
```





STRESS TEST

```
Context: default
Cluster: default
User: default
K9s Rev: v0.32.4
K8s Rev: v1.29.4+k3s1
CPU: 5%
MEM: 32%
```

```
<0> all      <ctrl-d> Delete
<1> deception <d>   Describe
<2> default    <e>   Edit
<?> Help
<y> YAML
```



Horizontalpodautoscalers(all)[1]

NAMESPACE↑	NAME	REFERENCE	TARGETS	MINPODS	MAXPODS	REPLICAS	AGE
monitoring	soc	Deployment/soc	8%/80%	1	100	11	3h40m

```
<horizontalpodautoscaler>
```

```
stages: [
  { duration: '10m', target: 200 }, // traffic ramp-up from 1 to a higher 200 users over 10 minutes.
  { duration: '30m', target: 200 }, // stay at higher 200 users for 30 minutes
  { duration: '5m', target: 0 }, // ramp-down to 0 users
],
```





BREAKPOINT TEST

```
Context: default
Cluster: default
User: default
K9s Rev: v0.32.4
K8s Rev: v1.29.4+k3s1
CPU: 15%
MEM: 42%
```

```
<0> all
<1> deception
<2> default
```



Horizontalpodautoscalers(all)[1]

NAMESPACE↑	NAME	REFERENCE	TARGETS	MINPODS	MAXPODS	REPLICAS	AGE
monitoring	soc	Deployment/soc	75%/80%	1	100	17	155m

<horizontalpodautoscaler>

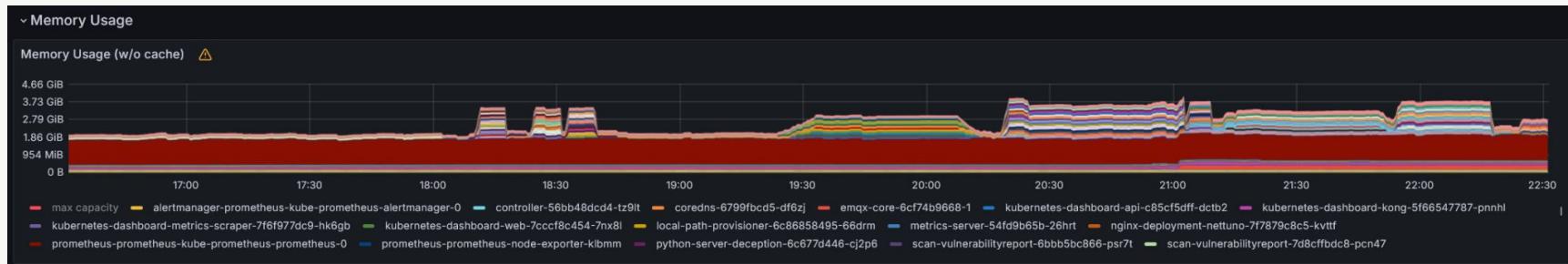
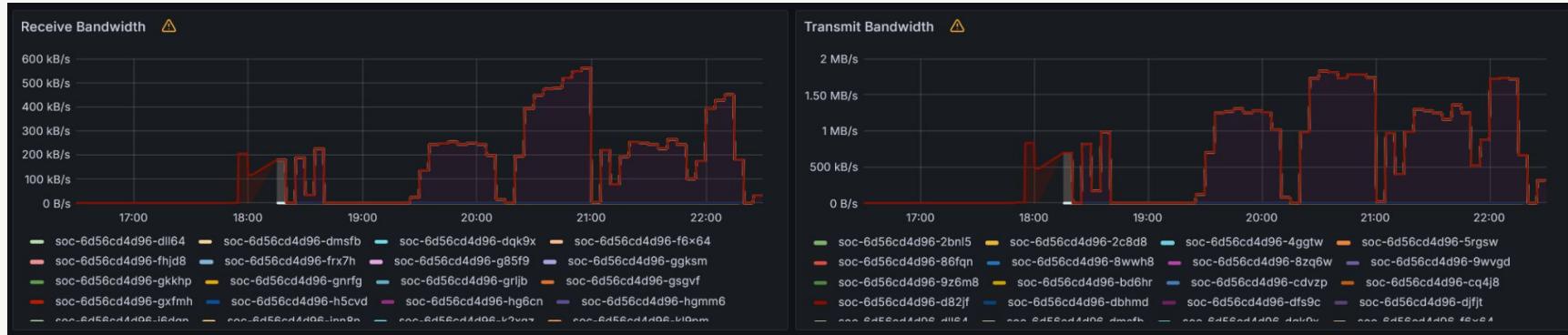
```
stages: [
  { duration: '2h', target: 20000 }, // just slowly ramp-up to a HUGE load
]
```



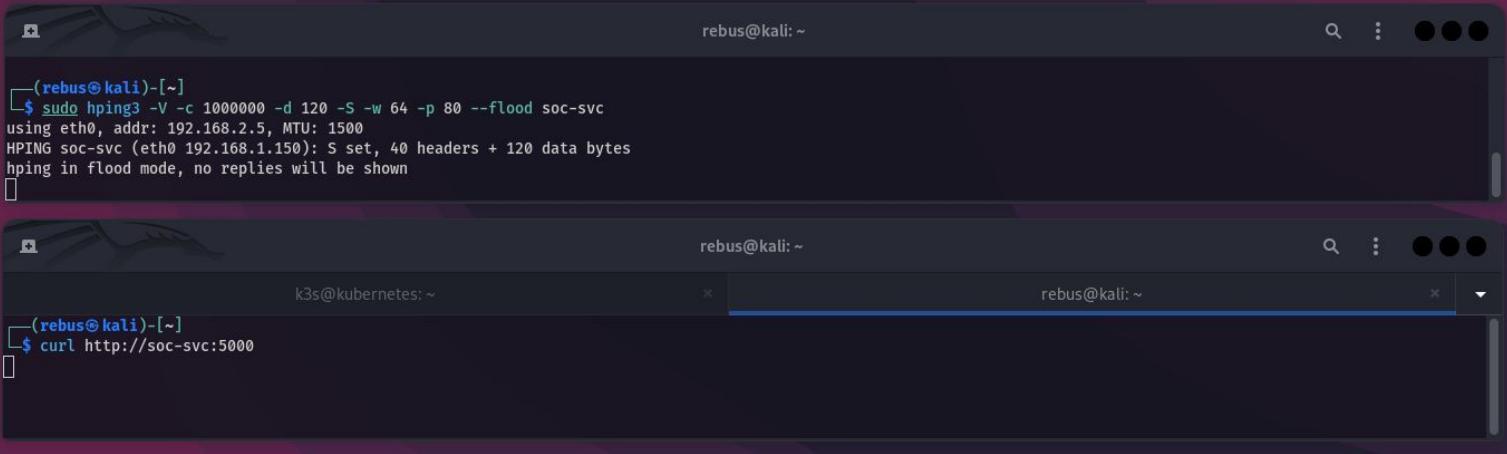
RESOURCES: CPU & MEMORY



RESOURCES: NETWORK & PODS



ATTACKS: DoS

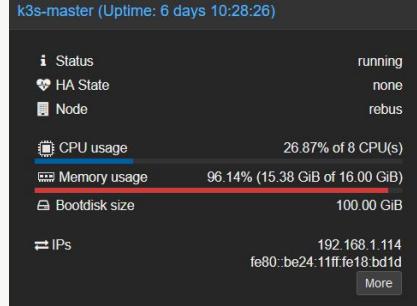
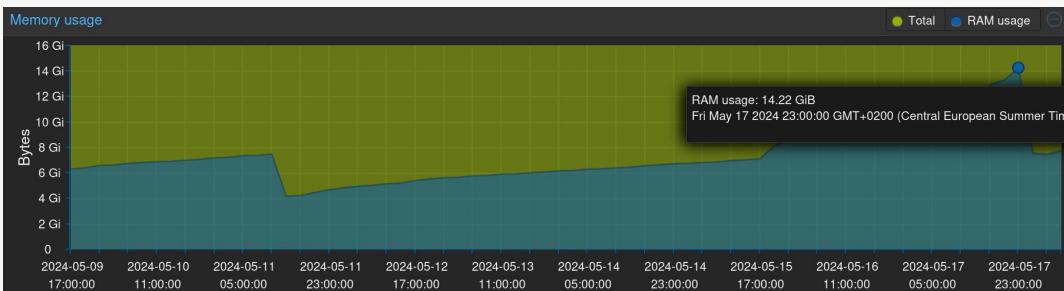


rebus@kali: ~

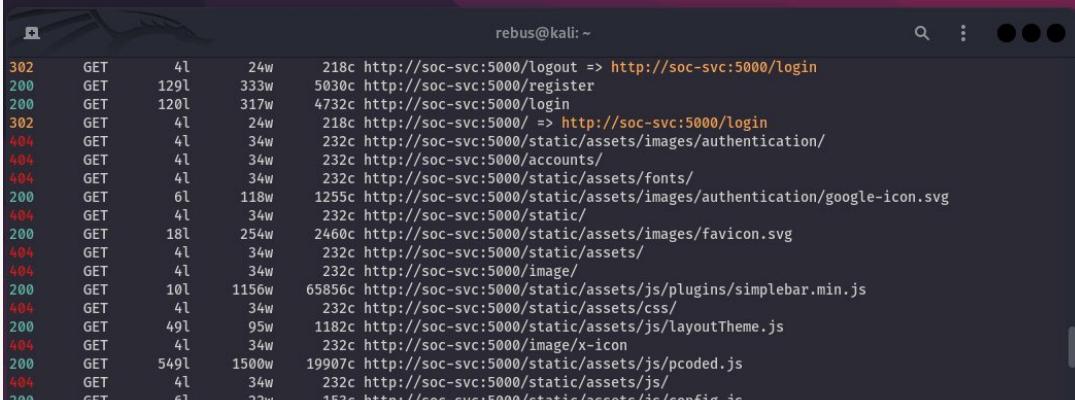
```
(rebus㉿kali)-[~]
$ sudo hping3 -V -c 1000000 -d 120 -S -w 64 -p 80 --flood soc-svc
using eth0, addr: 192.168.2.5, MTU: 1500
HPING soc-svc (eth0 192.168.1.150): S set, 40 headers + 120 data bytes
hping in flood mode, no replies will be shown
```

rebus@kali: ~

```
(rebus㉿kali)-[~]
$ curl http://soc-svc:5000
```

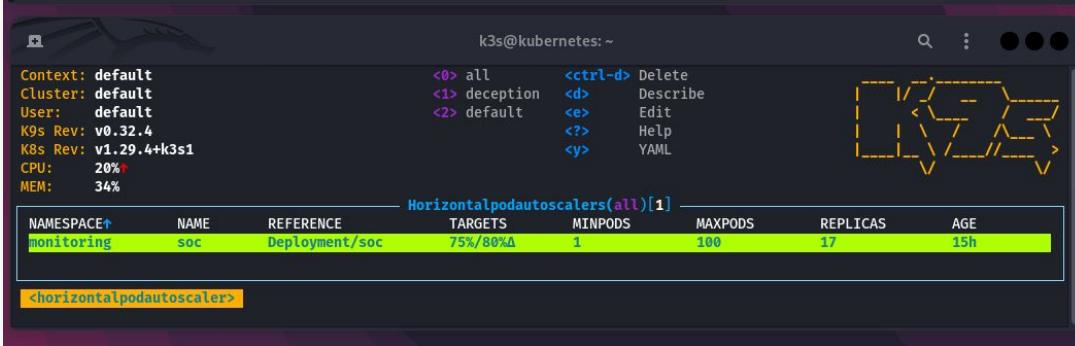


ATTACKS: Path Traversal



rebus@kali: ~

```
302 GET 4l 24w 218c http://soc-svc:5000/logout => http://soc-svc:5000/login
200 GET 129l 333w 5030c http://soc-svc:5000/register
200 GET 120l 317w 4732c http://soc-svc:5000/login
302 GET 4l 24w 218c http://soc-svc:5000/ => http://soc-svc:5000/login
404 GET 4l 34w 232c http://soc-svc:5000/static/assets/images/authentication/
404 GET 4l 34w 232c http://soc-svc:5000/accounts/
404 GET 4l 34w 232c http://soc-svc:5000/static/assets/fonts/
200 GET 6l 118w 1255c http://soc-svc:5000/static/assets/images/authentication/google-icon.svg
404 GET 4l 34w 232c http://soc-svc:5000/static/
200 GET 18l 254w 2460c http://soc-svc:5000/static/assets/images/favicon.svg
404 GET 4l 34w 232c http://soc-svc:5000/static/assets/
404 GET 4l 34w 232c http://soc-svc:5000/image/
200 GET 10l 1156w 65856c http://soc-svc:5000/static/assets/js/plugins/simplebar.min.js
404 GET 4l 34w 232c http://soc-svc:5000/static/assets/css/
200 GET 49l 95w 1182c http://soc-svc:5000/static/assets/js/layoutTheme.js
404 GET 4l 34w 232c http://soc-svc:5000/image/x-icon
200 GET 549l 1500w 19907c http://soc-svc:5000/static/assets/js/pcoded.js
404 GET 4l 34w 232c http://soc-svc:5000/static/assets/js/
200 GET 6l 22w 153c http://soc-svc:5000/static/assets/js/config.js
```

k3s@kubernetes: ~

```
Context: default          <0> all      <ctrl-d> Delete
Cluster: default          <1> deception <d> Describe
User: default              <2> default   <e> Edit
K9s Rev: v0.32.4           <?> Help
K8s Rev: v1.29.4+k3s1     <y> YAML
CPU: 20%*
MEM: 34%*
```

Horizontalpodautoscalers(all)[1]

NAMESPACE	NAME	REFERENCE	TARGETS	MINPODS	MAXPODS	REPLICAS	AGE
monitoring	soc	Deployment/soc	75%/80%	1	100	17	15h

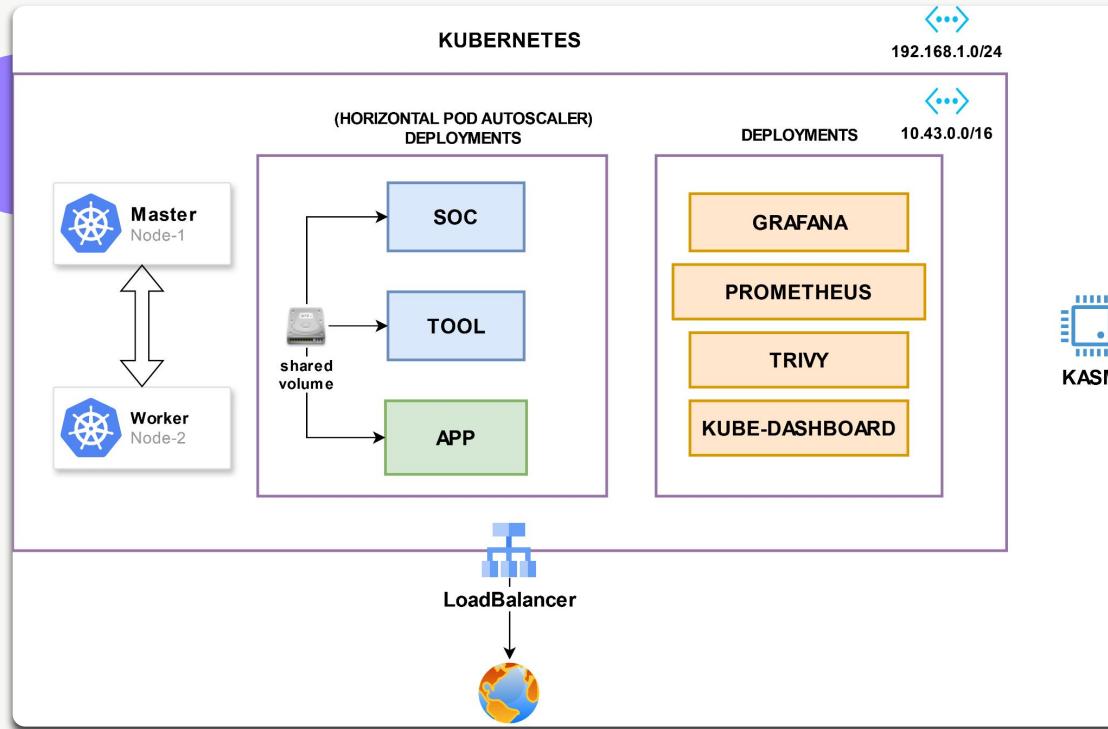
<horizontalpodautoscaler>

Risultati:

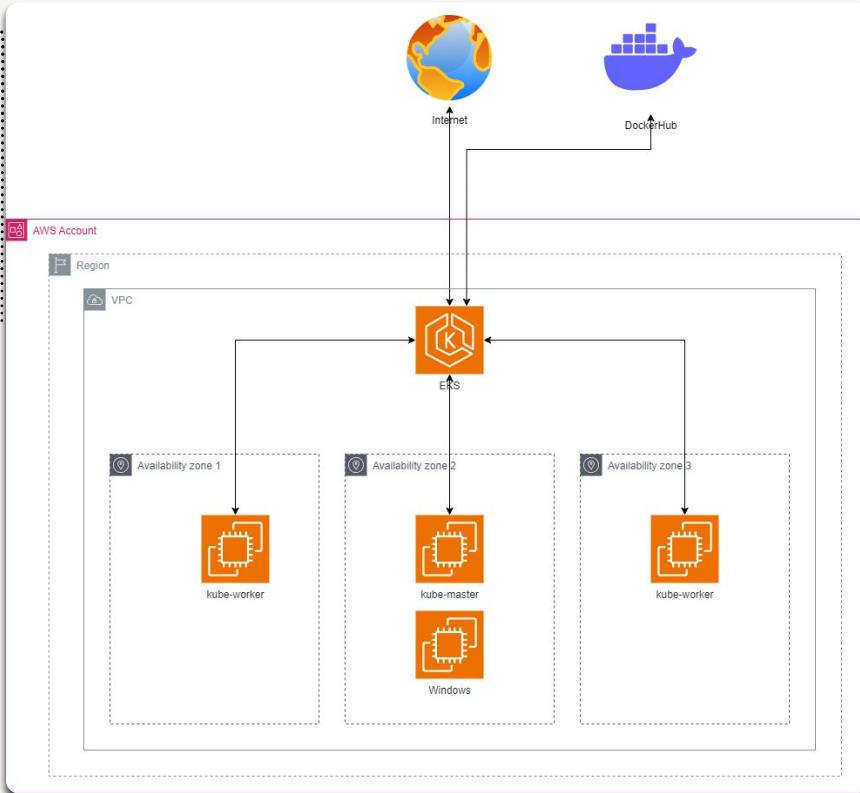
- Limite di 17 Pods per MS
- 1 Nodo con **16 GB Ram**,
CPU 12 core **3.7 GHz**
- NIC **1 Gb/s**

requests:
memory: "64Mi"
cpu: "100m"

DIAGRAMMA INFRASTRUTTURA



DISEGNO ARCHITETTURALE (AWS)



AUTOSCALING: NODI

EKS offre lo scaling orizzontale dei nodi master e worker

Autoscaling basato su metriche (es: CPU media utilizzata)

Nodi aggiunti o rimossi quando si supera una certa soglia di una certa metrica

Definizione di **minimi e massimi** desiderati

Efficienza economica grazie agli sprechi limitati



EKS > Clusters

Clusters (1) [Info](#)

Filter clusters

Cluster name	Status	Kubernetes version	Support period	Provider
eks-uX1OnQMw	Active	1.27 Upgrade now	⚠ Standard support until July 24, 2024	EKS

AUTOSCALING: NODI

Auto Scaling groups (2) Info								
<input type="checkbox"/>	Name	Launch template/configuration	Instances	Status	Desired capacity	Min	Max	Availability Zones
Create Auto Scaling group								
<input type="checkbox"/>	eks-node-group-1-20240525135140734800000019-90c7d802-be79-bed9-02ad-5a929ce5a929ce1ce7e	eks-90c7d802-be79-bed9-02ad-5a929ce	2	-	2	1	3	eu-central-1a, eu-central-1c, eu-central-1b
<input type="checkbox"/>	eks-node-group-2-2024052513514073600000001b-1cc7d802-be79-4fa4-3e67-80c1c863	eks-1cc7d802-be79-4fa4-3e67-80c1c863	1	-	1	1	2	eu-central-1a, eu-central-1c, eu-central-1b

AUTOSCALING: VOLUMI

EBS come fonte di storage per Kubernetes

Driver CSI per connettere Kubernetes a EBS

Scaling automatico quando si raggiunge una certa quantità di spazio utilizzato

NAME	PROVISIONER	RECLAIMPOLICY	VOLUMEBINDINGMODE	ALLOWVOLUMEEXPANSION	AGE
gp2 (default)	kubernetes.io/aws-ebs	Delete	WaitForFirstConsumer	false	82m
gp3 (default)	ebs.csi.aws.com	Retain	WaitForFirstConsumer	true	6m5s

NAMESPACE	NAME	READY	UP-TO-DATE	AVAILABLE	AGE
kube-system	coredns	2/2	2	2	79m
kube-system	ebs-csi-controller	2/2	2	2	77m
monitoring	prometheus-grafana	1/1	1	1	54m
monitoring	prometheus-kube-prometheus-operator	1/1	1	1	54m
monitoring	prometheus-kube-state-metrics	1/1	1	1	54m
monitoring	simple-app	1/1	1	1	40m
monitoring	soc	1/1	1	1	47m
monitoring	tool	1/1	1	1	46m
monitoring	trivy-operator	1/1	1	1	52m
monitoring	volume-autoscaler	1/1	1	1	9s

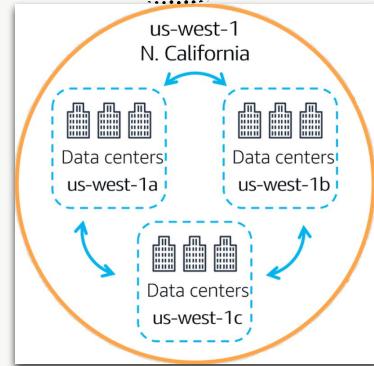
Volumes (3/3) Info						
<input type="text"/> Search						
<input checked="" type="checkbox"/> Name		<input checked="" type="checkbox"/> Volume ID		Type	Size	IOPS
<input checked="" type="checkbox"/>	node-group-1	vol-0092d53396e6c7a89	gp2	20 GiB	100	
<input checked="" type="checkbox"/>	node-group-2	vol-0a7bcb5a59c9a641b	gp2	20 GiB	100	
<input checked="" type="checkbox"/>	node-group-1	vol-04b020f5ba32bd209	gp2	20 GiB	100	

ALTA AFFIDABILITÀ: NODI

Separazione dei nodi in più **Availability Zones**

Availability Zone e Region: fault domain diversi

Separazione su più regioni non possibile con EKS



Instances (5) Info												
Connect Instance state Actions Launch instances												
<input type="text"/> Find Instance by attribute or tag (case-sensitive) All states												
	Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone	Public IPv4 DNS	Public IPv4 ...	Elastic IP		
<input type="checkbox"/>	node-group-1	I-07b2d44d4dd82995c	Running Q Q	t3.small	2/2 checks passed View alarms +	View alarms +	eu-central-1c	-	-	-		
<input type="checkbox"/>	ubuntu	I-04b8d5a44c302a9b8	Running Q Q	t2.micro	2/2 checks passed View alarms +	View alarms +	eu-central-1a	-	-	-		
<input type="checkbox"/>	windows	I-0f65f2fe494a5aea1	Running Q Q	t2.micro	2/2 checks passed View alarms +	View alarms +	eu-central-1a	-	-	-		
<input type="checkbox"/>	node-group-1	I-08c6aadcc6828b574	Running Q Q	t3.small	2/2 checks passed View alarms +	View alarms +	eu-central-1b	-	-	-		
<input type="checkbox"/>	node-group-2	I-0c3f93ed70e743ac0	Running Q Q	t3.small	2/2 checks passed View alarms +	View alarms +	eu-central-1a	-	-	-		

ALTA AFFIDABILITÀ: RETE

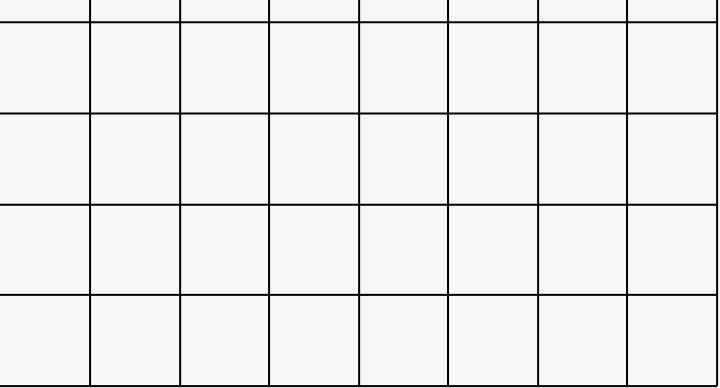
Subnets (6) Info					
<input type="text"/> Find resources by attribute or tag					
<input type="checkbox"/>	Name	Subnet ID	State	VPC	IPv4 CIDR
<input type="checkbox"/>	eks-srs-vpc-private-eu-central-1a	subnet-0247f63d109338542	✓ Available	vpc-047b7d8cb3ab51a2c eks-...	10.8.1.0/24
<input type="checkbox"/>	eks-srs-vpc-public-eu-central-1a	subnet-0eb509617973ac135	✓ Available	vpc-047b7d8cb3ab51a2c eks-...	10.8.4.0/24
<input type="checkbox"/>	eks-srs-vpc-private-eu-central-1b	subnet-07a43e4db2b2b3d1c	✓ Available	vpc-047b7d8cb3ab51a2c eks-...	10.8.2.0/24
<input type="checkbox"/>	eks-srs-vpc-public-eu-central-1b	subnet-0ffb5b992f877f2a8	✓ Available	vpc-047b7d8cb3ab51a2c eks-...	10.8.5.0/24
<input type="checkbox"/>	eks-srs-vpc-public-eu-central-1c	subnet-08dab65a7558fffd3	✓ Available	vpc-047b7d8cb3ab51a2c eks-...	10.8.6.0/24
<input type="checkbox"/>	eks-srs-vpc-private-eu-central-1c	subnet-0cb10ee8285d45ae0	✓ Available	vpc-047b7d8cb3ab51a2c eks-...	10.8.3.0/24

MINISOC on AWS

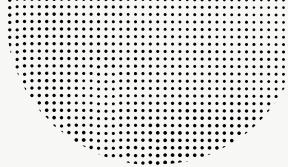
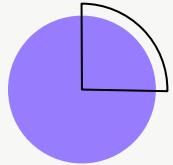
The screenshot shows a web browser window with the URL `ab4836cbe029d40c08d899261dbb8b97-1259281123.eu-central-1.elb.amazonaws.com:5000/index`. The page has a dark theme with purple accents. On the left is a sidebar menu:

- Dashboard**
 - Home
 - Cluster
- Security**
 - Network Analyzer
 - Malware Analyzer
 - Kasm
- Statistics**
 - CoreDNS
 - Pods Workload - Master
 - Pods Workload - Worker
 - Volumes
 - Networking
 - Application Statistics
 - Trivy

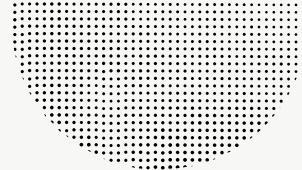
The main content area features a large, stylized "MiniSOC" logo in purple. At the bottom of the page, there is footer text: "© FlippaFioppa - Coded by BlessedRebuS, leonardobambini, RootLe00." and "The GNU General Public License v3.0".



DEMO



<https://github.com/FlippaFloppa/MINISOC>



GRAZIE PER L'ATTENZIONE



Bambini Leonardo
Leonelli Caterina
Di Fazio Patrick