radware

Radware KWAAP - SUSE Rancher Prime Integration

Raphael Chileshe

Senior Security Solution Architect/Appsec/Cloud Native

February 2025

What is SUSE Rancher Prime?

- **SUSE Rancher Prime** is a Kubernetes management platform to deploy and run clusters anywhere and on any provider. SUSE Rancher Prime provides the ability to provision Kubernetes from a hosted provider, provision compute nodes and then install Kubernetes onto them, or import existing Kubernetes clusters running anywhere.
- **SUSE Rancher Prime** adds significant value on top of Kubernetes, first by centralizing authentication and role-based access control (RBAC) for all of the clusters, giving global admins the ability to control cluster access from one location.
- It then enables detailed monitoring and alerting for clusters and their resources, ships logs to external providers, and integrates directly with Helm via the Application Catalog. If you have an external CI/CD system, you can plug it into **SUSE Rancher Prime**, but if you don't, **SUSE Rancher Prime** even includes Fleet to help you automatically deploy and upgrade workloads.
- **SUSE Rancher Prime** is a *complete* container management platform for Kubernetes, giving you the tools to successfully run Kubernetes anywhere.
  https://www.suse.com/products/rancher/

SUSE Rancher Kubernetes Engine (RKE2)

- SUSE Rancher Kubernetes Engine (RKE2) is a CNCF-certified Kubernetes distribution that runs entirely within Docker containers. It works on bare-metal and virtualized servers. RKE2 solves the problem of installation complexity, a common issue in the Kubernetes community. With RKE2, the installation and operation of Kubernetes is both simplified and easily automated, and it's entirely independent of the operating system and platform you're running. As long as you can run a supported version of Docker, you can deploy and run Kubernetes with RKE2.

  https://documentation.suse.com/cloudnative/rke2/

What Does Radware Kubernetes WAAP Do?

- Radware Kubernetes Web Application and API Protection (KWAAP) is a comprehensive and highly scalable Web application security solution for CI/CD environments orchestrated by Kubernetes. In addition to market leading data and application protection, Radware Kubernetes WAAP is designed to natively fit these environments, meeting the required levels of automation, flexibility and elasticity.
- The solution easily integrates with common software provisioning, testing and visibility tools in the CI/CD pipeline offering both IT security and DevOps personnel detailed insight down to the pod and container levels, and enables organizations to implement effective application and data security in on-premise and cloud-based implementations.
  - OWASP Top 10 API Coverage
  - OWASP Top 10 Web Application Protection
  - DLP
  - Behavioral Based Application security
  - Response based tracking features
  - File based protection
  - Rate-limiting features

High-level Environment Setup

- Deploy a **3 Node Cluster on rke2** managed by Rancher server
- Integrate **Private Image Registry** into Rancher Server
- Deploy Radware KWAAP Advanced Application security protection Control Plane within RKE in namespace KWAAP
- Deploy Vulnerable applications in their own namespace unprotected with RKE managed by rancher server
- Patch the vulnerable apps with KWAAP enforce to protect the apps
- Configure an application security policy for the apps
- Deploying the following apps in rancher:
  - Neuvector (Security Compliance)
  - CIS Benchmark (Security Compliance)
  - Grafana (Monitoring)

SUSE Rancher Prime Server and RKE2 Deployment

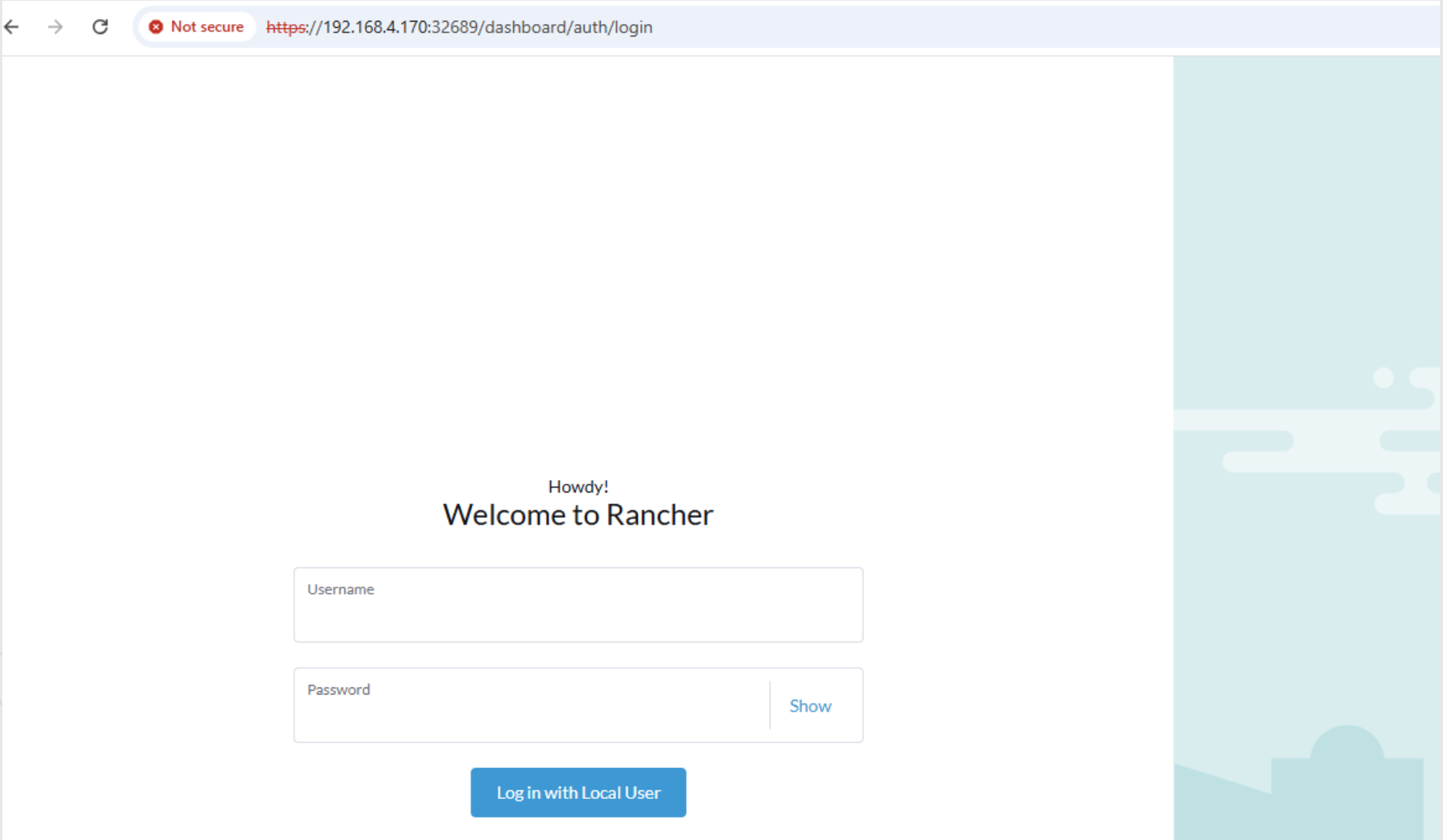
- RKE2 Deployment

```
root@suse04170:~# kubectl get node
NAME                    STATUS   ROLES                       AGE   VERSION
suse04170.intrusis.io   Ready    control-plane,etcd,master   8h    v1.31.5+rke2r1
suse04171.intrusis.io   Ready    <none>                      8h    v1.31.5+rke2r1
suse04172.intrusis.io   Ready    <none>                      8h    v1.31.5+rke2r1
root@suse04170:~#
```

- SUSE Rancher Prime Server management

```
root@suse04170:~# kubectl get node
NAME                    STATUS   ROLES                       AGE   VERSION
suse04170.intrusis.io   Ready    control-plane,etcd,master   8h    v1.31.5+rke2r1
suse04171.intrusis.io   Ready    <none>                      8h    v1.31.5+rke2r1
suse04172.intrusis.io   Ready    <none>                      8h    v1.31.5+rke2r1
root@suse04170:~# kubectl get svc -n cattle-system
NAME              TYPE        CLUSTER-IP      EXTERNAL-IP   PORT(S)                      AGE
rancher           NodePort    10.43.241.109   <none>        80:31489/TCP,443:32689/TCP   7h8m
rancher-webhook   ClusterIP   10.43.254.57    <none>        443/TCP                      7h5m
root@suse04170:~#
```

SUSE Rancher Prime Server and RKE2 Deployment



SUSE Rancher Prime Server and RKE2 Deployment

Not secure https://192.168.4.170:32689/dashboard/c/local/explorer/node

local

All Namespaces

Cluster
- Projects/Namespaces
- Nodes 3
- Cluster and Project Members
- Events 10
- Tools

Workloads
Apps
Service Discovery
Storage
Policy
Monitoring
CIS Benchmark
NeuVector
More Resources

The base Kubernetes Node resource represents a virtual or physical machine which hosts deployments. To manage the machine lifecycle, if available, go to Cluster Management.

Nodes

Download YAML | Delete | Filter

State	Name	Roles	Version	External/Internal IP	OS	CPU	RAM	Pods	Age
Active	suse04170.intrusis.io	Control Plane, Etcd	v1.31.5+rke2r1	- / 192.168.4.170	Linux	9.4%	51%	25%	3.9 days
Active	suse04171.intrusis.io	Worker	v1.31.5+rke2r1	- / 192.168.4.171	Linux	24%	58%	25%	3.9 days
Active	suse04172.intrusis.io	Worker	v1.31.5+rke2r1	- / 192.168.4.172	Linux	7.1%	62%	23%	3.9 days

```
root@suse04170:~# kubectl get node -o wide
NAME                  STATUS   ROLES                       AGE   VERSION          INTERNAL-IP     EXTERNAL-IP   OS-IMAGE           KERNEL-VERSION     CONTAINER-RUNTIME
suse04170.intrusis.io Ready    control-plane,etcd,master   8h    v1.31.5+rke2r1   192.168.4.170   <none>        Ubuntu 24.04 LTS   6.8.0-31-generic   containerd://1.7.23-k3s2
suse04171.intrusis.io Ready    <none>                      8h    v1.31.5+rke2r1   192.168.4.171   <none>        Ubuntu 24.04 LTS   6.8.0-31-generic   containerd://1.7.23-k3s2
suse04172.intrusis.io Ready    <none>                      8h    v1.31.5+rke2r1   192.168.4.172   <none>        Ubuntu 24.04 LTS   6.8.0-31-generic   containerd://1.7.23-k3s2
root@suse04170:~#
```

Radware KWAAP Deployment Control Plane

Not secure https://192.168.4.170:32689/dashboard/c/local/explorer/workload

local

kwaf

Cluster
Workloads
CronJobs 1
DaemonSets 0
Deployments 7
Jobs 1
StatefulSets 2
Pods 10
Apps
Service Discovery
Storage
Policy
Monitoring
CIS Benchmark
NeuVector
More Resources

Workloads

Create

Redeploy | Run Now | Suspend | Download YAML | Delete

Filter

State	Name	Namespace	Type	Image	Restarts	Age	Health
Active	waas-controller-deployment	kwaf	Deployment	dockreg.intrusis.io:8443/waas-controller:1.19.0	0	1 hour	
Active	waas-elasticsearch-deployment	kwaf	StatefulSet	dockreg.intrusis.io:8443/waas-elasticsearch:1.19.0	0	1 hour	
Active	waas-events-fetcher-deployment	kwaf	Deployment	dockreg.intrusis.io:8443/waas-events-fetcher:1.19.0	0	1 hour	
Active	waas-gui-deployment	kwaf	Deployment	dockreg.intrusis.io:8443/waas-gui:1.19.0 + 1 more	0	1 hour	
Active	waas-license-meter-job	kwaf	CronJob	dockreg.intrusis.io:8443/waas-license-meter:1.19.0	0	1 hour	
Active	waas-logstash-deployment	kwaf	Deployment	dockreg.intrusis.io:8443/waas-logstash:1.19.0	0	1 hour	
Active	waas-profiles-crud-deployment	kwaf	Deployment	dockreg.intrusis.io:8443/waas-profiles-crud:1.19.0	0	1 hour	
Active	waas-rate-limiter-deployment	kwaf	Deployment	dockreg.intrusis.io:8443/waas-rate-limiter:1.19.0	0	1 hour	
Active	waas-redis-statefulset	kwaf	StatefulSet	dockreg.intrusis.io:8443/waas-redis-exporter:1.19.0 + 1 more	0	1 hour	
Active	waas-validation-controller-deployment	kwaf	Deployment	dockreg.intrusis.io:8443/waas-validationcontroller:1.19.0	0	1 hour	

Radware KWAAP Management UI

Not secure https://192.168.4.170:32689/dashboard/c/local/explorer/apps.deployment/kwaf/waas-gui-deployment#services

local

kwaf

- Cluster
- Workloads
  - CronJobs 1
  - DaemonSets 0
  - Deployments 7
  - Jobs 1
  - StatefulSets 2
  - Pods 10
- Apps
- Service Discovery
- Storage
- Policy
- Monitoring
- CIS Benchmark
- NeuVector
- More Resources

Deployment: waas-gui-deployment Active

Namespace: kwaf Age: 1 hour Pod Restarts: 0

Detail Config YAML

Image: dockreg.intrusis.io:8443/waas-gui:1.19.0 Ready: 1/1 Up-to-date: 1 Available: 1
+ 1 more

Endpoints: [Any Node]:31005

Labels: app.kubernetes.io/instance : WAAS app.kubernetes.io/managed-by : Helm app.kubernetes.io/name : WAAS

Annotations: Show 3 annotations

Pods by State

Scale 1

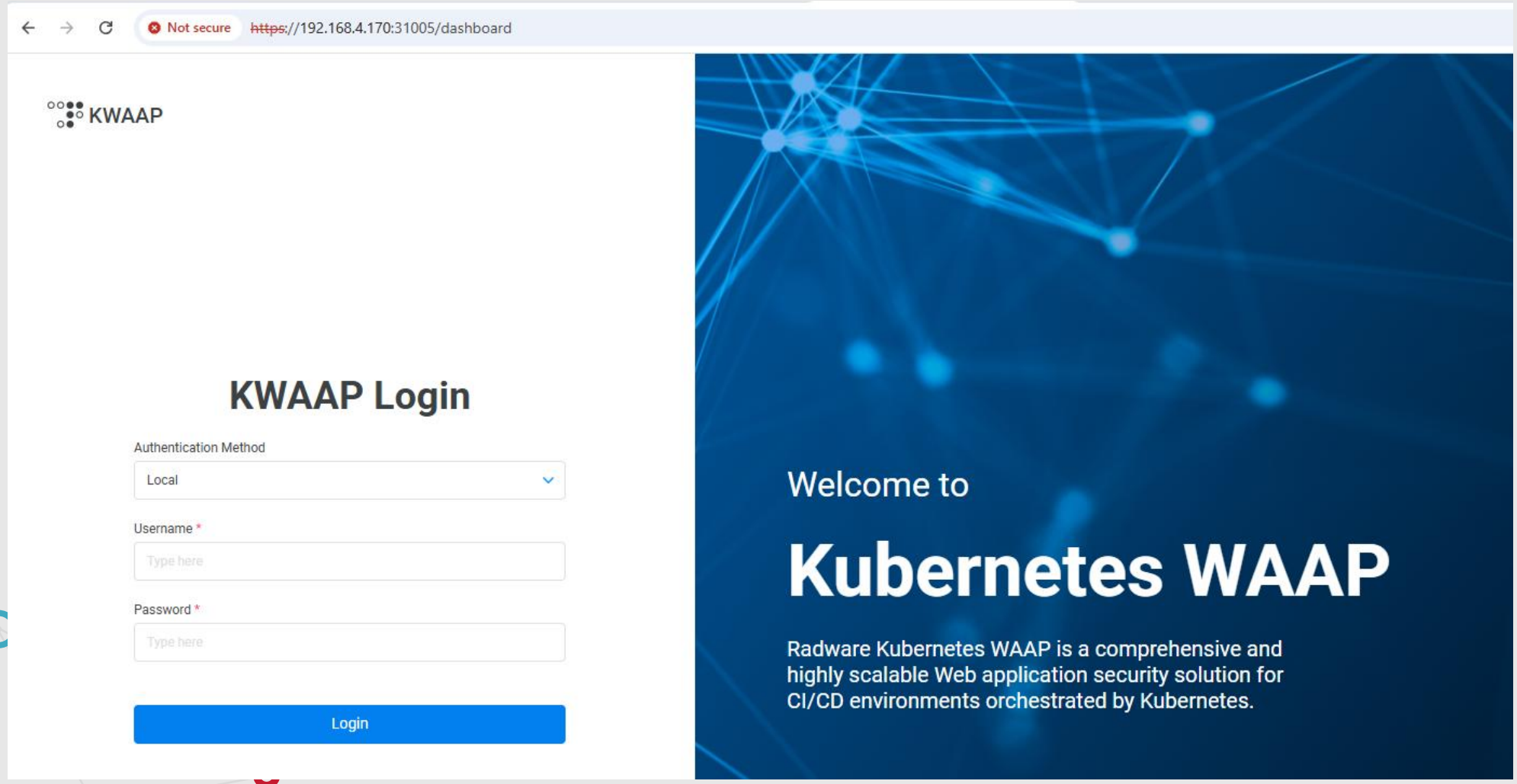
1
Running

Pods Metrics Services Ingresses Conditions Recent Events Related Resources

The following Services select Pods from this workload:

State	Name	Namespace	Target	Selector	Type	Age
Active	waas-gui	kwaf	[Any Node]:31005	configid=waas-gui-container	Node Port	1 hour

Radware KWAAP Management UI



Runtime Vulnerable Apps Deployment in RKE2

Not secure https://192.168.4.170:32689/dashboard/c/local/explorer/apps.deployment

local

kwaap-inline-altorom ✕ +2

Cluster
Workloads
CronJobs 0
DaemonSets 0
Deployments 3
Jobs 0
StatefulSets 0
Pods 3
Apps
Service Discovery
Storage
Policy
Monitoring
CIS Benchmark
NeuVector
More Resources

Deployments

Create

Redeploy | Download YAML | Delete

Filter

State	Name	Image	Ready	Up To Date	Available	Restarts	Age	Health
Namespace: kwaap-inline-altorom								
Active	sample-altorom-deployment	dockreg.intrusis.io:8443/waas-bootstrap:1.19.0 + 3 more	1/1	1	1	0	39 mins	
Namespace: kwaap-inline-bwapp								
Active	sample-bwapp-deployment	dockreg.intrusis.io:8443/waas-bootstrap:1.19.0 + 3 more	1/1	1	1	0	56 mins	
Namespace: kwaap-inline-hackazon								
Active	sample-hackazon-deployment	dockreg.intrusis.io:8443/waas-bootstrap:1.19.0 + 3 more	1/1	1	1	0	36 mins	

Application with KWAAP Enforcer as Sidecar Container

Not secure https://192.168.4.170:32689/dashboard/c/local/explorer/pod/kwaap-inline-altorom/sample-altorom-deployment-85c8d48cc7-7mrbx#containers

local

kwaap-inline-altorom +2

Cluster
Workloads
CronJobs 0
DaemonSets 0
Deployments 3
Jobs 0
StatefulSets 0
Pods 3
Apps
Service Discovery
Storage
Policy
Monitoring
CIS Benchmark
NeuVector
More Resources

Pod: sample-altorom-deployment-85c8d48cc7-7mrbx Running
Namespace: kwaap-inline-altorom Age: 40 mins

APPLICATION POD

Detail Config YAML

Pod IP: 10.42.2.30 Workload: sample-altorom-deployment-85c8d48cc7 Node: suse04171.intrusis.io
Labels: app : sample-altorom-container pod-template-hash : 85c8d48cc7 waas.radware.com/protection : enabled
Annotations: Show 3 annotations

Containers Metrics Conditions Recent Events Related Resources

State	Ready	Name	Image		Init Container	Restarts	Started	
Running	✓	enforcer	dockreg.intrusis.io:8443/waas-bootstrap:1.19.0	KWAF ENFORCER SIDECAR CONTAINER	—	0	40 mins ago	
Running	✓	fluentbit	dockreg.intrusis.io:8443/waas-fluentbit:1.19.0		—	0	40 mins ago	
Terminated Completed	✓	init-enrich	dockreg.intrusis.io:8443/waas-enrich:499		✓	0	-	
Running	✓	logrotate	dockreg.intrusis.io:8443/waas-logrotate:1.19.0		—	0	40 mins ago	
Running	✓	sample-altorom	dockreg.intrusis.io:8443/altoromutuals:latest	APPLICATION CONTAINER	—	0	40 mins ago	

Accessing Application through RKE2 using NodePort

Not secure https://192.168.4.170:32689/dashboard/c/local/explorer/apps.deployment/kwaap-inline-altorom/sample-altorom-deployment#services

local | kwaap-inline-altorom | +2

Cluster
Workloads
CronJobs 0
DaemonSets 0
Deployments 3
Jobs 0
StatefulSets 0
Pods 3
Apps
Service Discovery
Storage
Policy
Monitoring
CIS Benchmark
NeuVector
More Resources

Deployment: sample-altorom-deployment Active
Namespace: kwaap-inline-altorom Age: 43 mins Pod Restarts: 0

Detail Config YAML

Image: dockreg.intrusis.io:8443/waas-bootstrap:1.19.0 Ready: 1/1 Up-to-date: 1 Available: 1
+ 3 more
Endpoints: [Any Node]:31021
Labels: waas.radware.com/sample : altorom
Annotations: Show 2 annotations

Pods by State

Scale 1

1
Running

Pods

local | kwaap-inline-hackazon

Cluster
Workloads
Apps
Service Discovery
HorizontalPodAutoscalers 0
Ingresses 1
Services 12
Storage
Policy
Monitoring

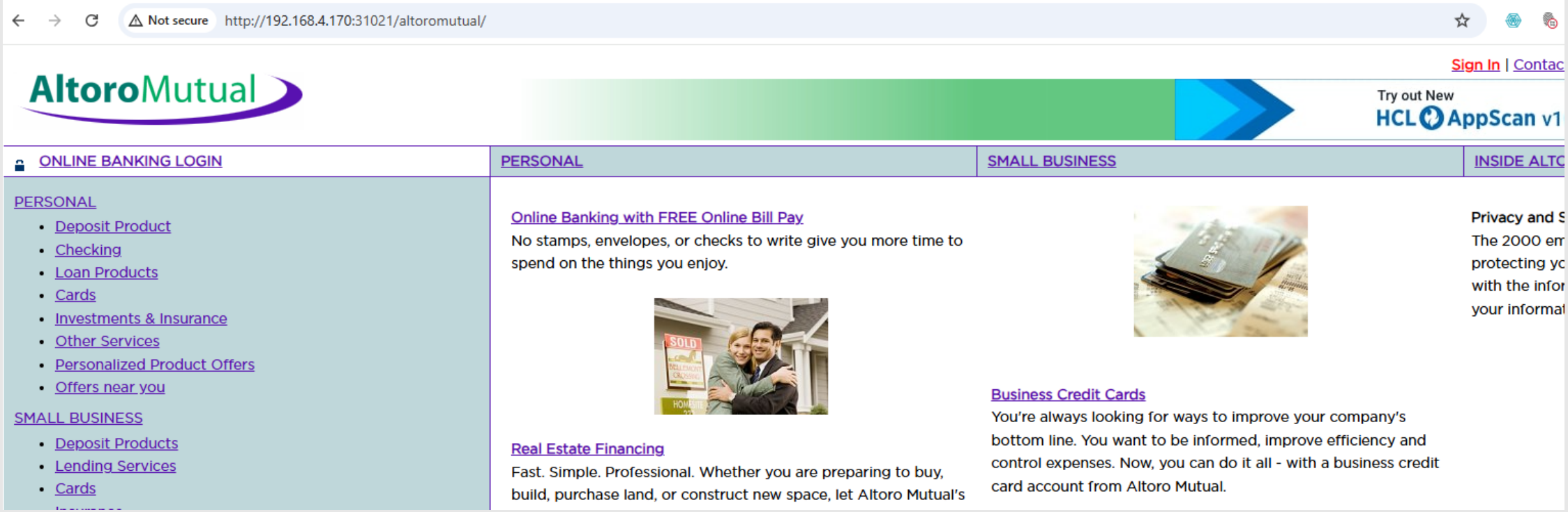
Service: sample-altorom-service Active
Namespace: kwaap-inline-altorom Age: 3.6 days

Type: NodePort Cluster IP: 10.43.202.128 Session Affinity: None
Labels: waas.radware.com/sample : altorom
Annotations: Show 1 annotation

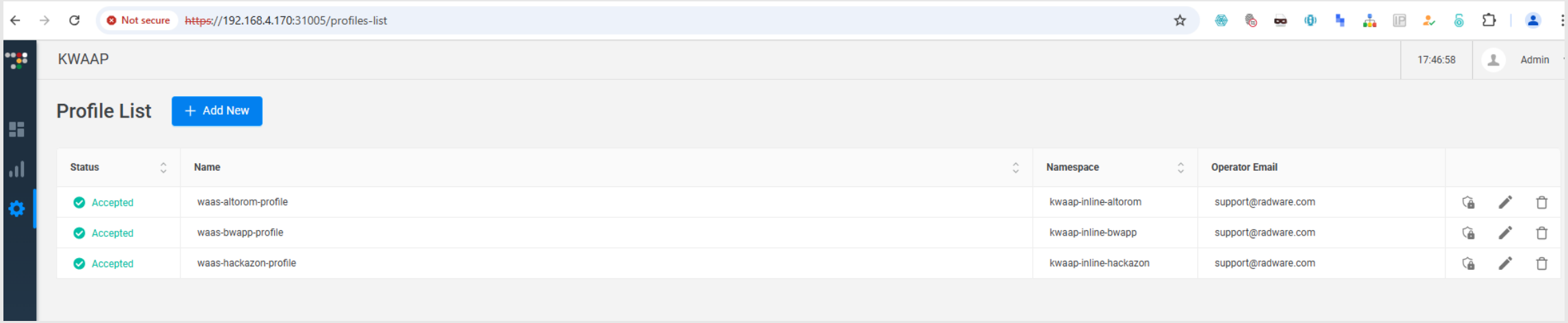
Pods | Ports | Selectors | Conditions | Recent Events | Related Resources

Name	Port	Protocol	Target	Node Port
http	80	TCP	9000	31021

Accessing Application through RKE2 using NodePort



Radware KWAAP Security Policy Configuration



Radware KWAAP Protection Modules

Edit Protection

Applied on Classifiers

altorom-sample

Protections

Protection ID *

altorom

Global Protection Action

Inspect

Custom HTTP Response Code

Type Here

Custom HTTP Response Code Override

RFC Validation | Signatures Engine | Expressions Engine | Access Control | DLP | **Activity Tracking** | API Security | Patterns | JWT | Response Tracking | Actor Anomalies | File Upload | Violation Rating

Activity Tracking

Bypass

Report Mode

All

Static Resources

Include only requests with p...

Blocking Cache Strategy

Any

Custom HTTP Response Code

Add Retry-After Response Header

Source IP

+ Add Actor

Rate Limit *

5 Per: Second

Rate Sync Frequency *

1

Blocking Time *

5 Minute

Blocking Cache *

Radware KWAAP Protection Modules

- RFC Validation
- Signature Engine
- Expression Engine
- Access Control
- DLP
- Activity Tracking
- API Security
- Patterns
- JWT
- Response Tracking
- Actor Anomalies
- File Upload Violation Rating

SQL Injection Simple Test

Not secure http://192.168.4.170:31021/altoromutual/login.jsp

AltoroMutual

New

ONLINE BANKING LOGIN | PERSONAL | SMALL BUSINESS

PERSONAL
- Deposit Product
- Checking
- Loan Products
- Cards
- Investments & Insurance
- Other Services
- Personalized Product Offers
- Offers near you

SMALL BUSINESS
- Deposit Products

Online Banking Login

Username: 'or 1=1--

Password: •••••

Login

Not secure http://192.168.4.170:31021/altoromutual/doLogin

This XML file does not appear to have any style information associated with it. The document tree is shown below.


```
▼<root>
  <Response>Unauthorized Activity Has Been Detected</Response>
  <Reason>You are seeing this because we have detected unauthorized activity. If you believe that there has been some mistake, please send an e-mail to our Web site security team at support@radware.com with the following case number as the subject: Case ID:
  f8951656-e79f-42e7-97c8-2c0abe6b48f3</Reason>
  <Date>2025-02-06T22:48:53.796Z</Date>
  <CaseNumber>f8951656-e79f-42e7-97c8-2c0abe6b48f3</CaseNumber>
  <OperatorEmail>support@radware.com</OperatorEmail>
</root>
```

Detection and Reporting

Not secure https://192.168.4.170:31005/security-events?startDateISO=now-15m&endDateISO=now&operator=AND

KWAAP | 17:50:00 | Admin

Security Events

Switch to Custom

Search | Apply | AND | OR | Filters... | Clear All | 15m | Refresh

Fields Summary

KWAAP configuration

Tags:	1	Profiles:	1
Classifiers:	1	Modules:	1

Attack Details

Actions:	1	Attacks Name:	1
Severities:	1	Threats Name:	2
Titles:	1	Signatures Version:	1
Patterns:	0	Signatures:	3
Zones:	1	OWASP Violations:	1

Client parameter

Locations:	0	Real IP Address:	0
Real IP Header:	0	User Agent:	1

Request

Hostnames:	1	Parameters Name:	1
Headers Name:	0	Parameters Value:	1
Headers Value:	0	URIs:	1
Methods:	1		

Security Events by Action

Total: 3

3 Blocked Events

Security Events

Export Selected | Export All

Action	Time & Date	Severity	Client Source	Location	Hostname	Threat	Attack Name	Module
Blocked	06-02-25 17:48:53	|||||	10.42.0.0:58608	N/A	192.168.4.170:31021	SQL Threat	SQL Injection	Known Attacks - Expressio...

Client Parameter

Location:	-	Real IP Header:	-
Real IP Address:	-	User-Agent:	Mozilla/5.0 (Wi...
Source IP:	10.42.0.0:58608	Proxy:	-

Request

Hostname:	192.168.4.170:...	URI:	/altoromutual/...
Method:	POST	Cookie:	JSESSIONID=A...
Referer:	http://192.168....	Content-type:	application/x-...

Attack Details

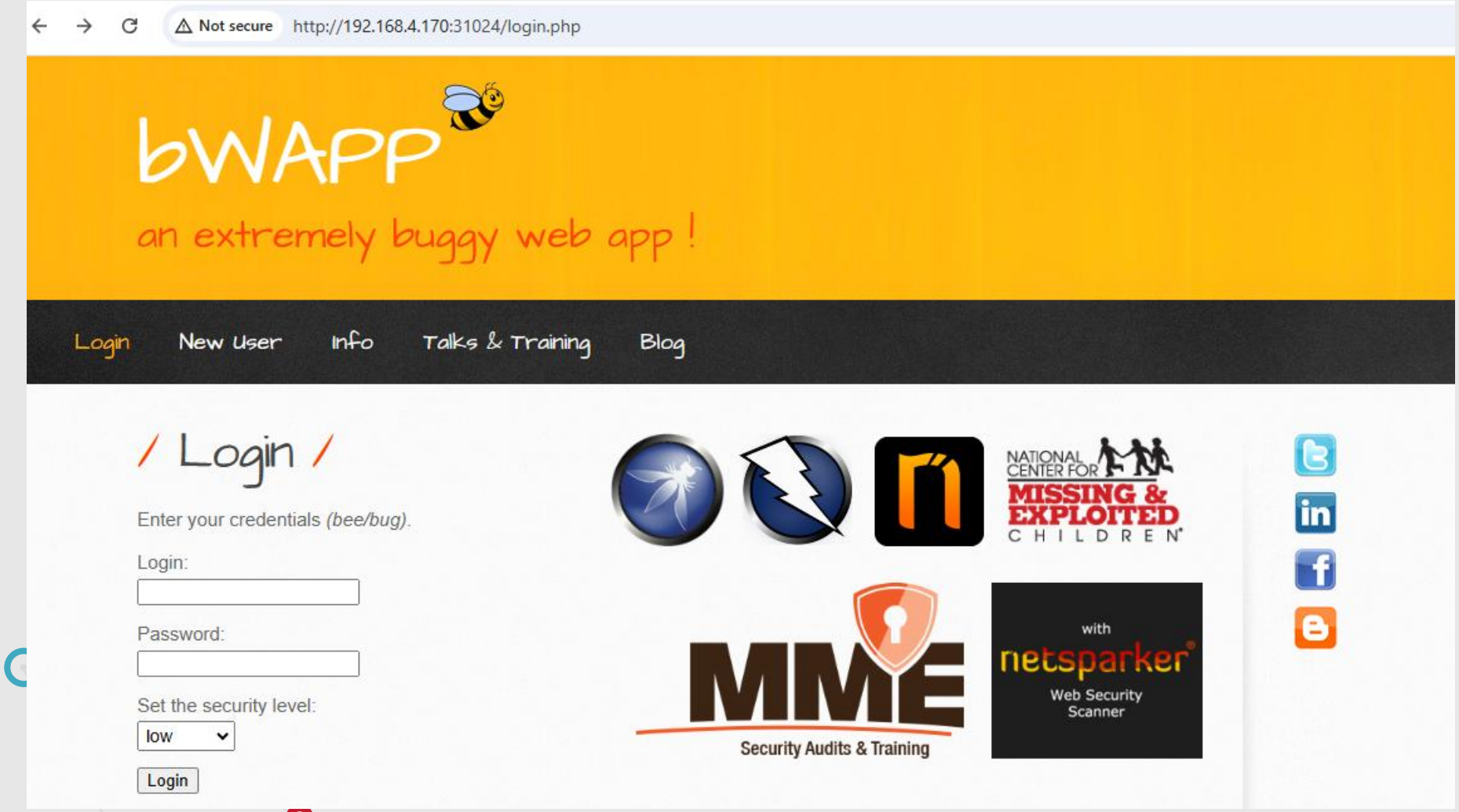
Action:	Blocked	Violation Penalty:	-
Transaction ID:	f8951656-e79f...	Title:	Parameter Vali...
Threat Name:	SQL Threat	Attack Name:	SQL Injection
Severity Level:	High	OWASP Violation:	A3-2021: Inject...
Version:	8.0.0.499 - Dec...	CVE:	-
Pattern:	-	Signature:	LFISRT
Details:	An attempt ha...	Example:	MyColumn=My...
Type:	-	Zone:	Parameters
Parameter Type:	Body	Violation Details:	-
Encoding:	Url	Encoded Values:	'or 1=1-- , %27o...

KWAAP Configuration

Description

Expression engine intercepted a malicious request with a submitted Parameter value, which includes a harmful expression. No description

Simple WAAP Test



Detection and Reporting

Not secure http://192.168.4.170:31024/login.php/etc/passwd

Unauthorized Activity Has Been Detected

radware

You are seeing this page because we have detected unauthorized activity.
If you believe that there has been some mistake,please send an e-mail to our Web site security team at support@radware.com
with the following case number as the subject: *Case ID: 58369d73-bbd2-483a-9f21-56d155eb7373.*

Date:	Thursday, February 6, 2025 at 5:52:11 PM
Case Number:	58369d73-bbd2-483a-9f21-56d155eb7373
Operator email:	support@radware.com

Detection and Reporting

Not secure https://192.168.4.170:31005/security-events?startDateISO=now-15m&endDateISO=now&operator=AND

KWAAP | 17:53:07 | Admin

Security Events

Switch to Custom

Search | Apply | AND | OR | Filters... | Clear All | 15m | Refresh

Fields Summary

KWAAP configuration

Tags:	1	Profiles:	2
Classifiers:	2	Modules:	2

Attack Details

Actions:	1	Attacks Name:	3
Severities:	2	Threats Name:	4
Titles:	2	Signatures Version:	1
Patterns:	2	Signatures:	5
Zones:	2	OWASP Violations:	3

Client parameter

Locations:	0	Real IP Address:	0
Real IP Header:	0	User Agent:	1

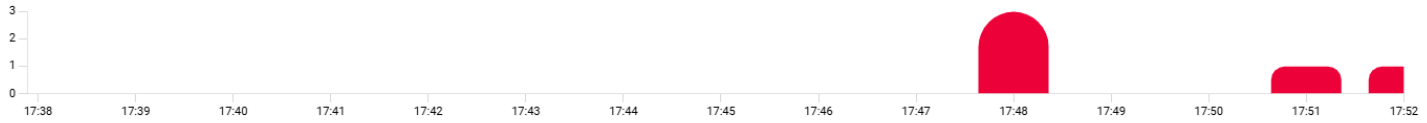
Request

Hostnames:	2	Parameters Name:	1
Headers Name:	0	Parameters Value:	1
Headers Value:	0	URIs:	3

Security Events by Action

Total: 5

5 Blocked Events

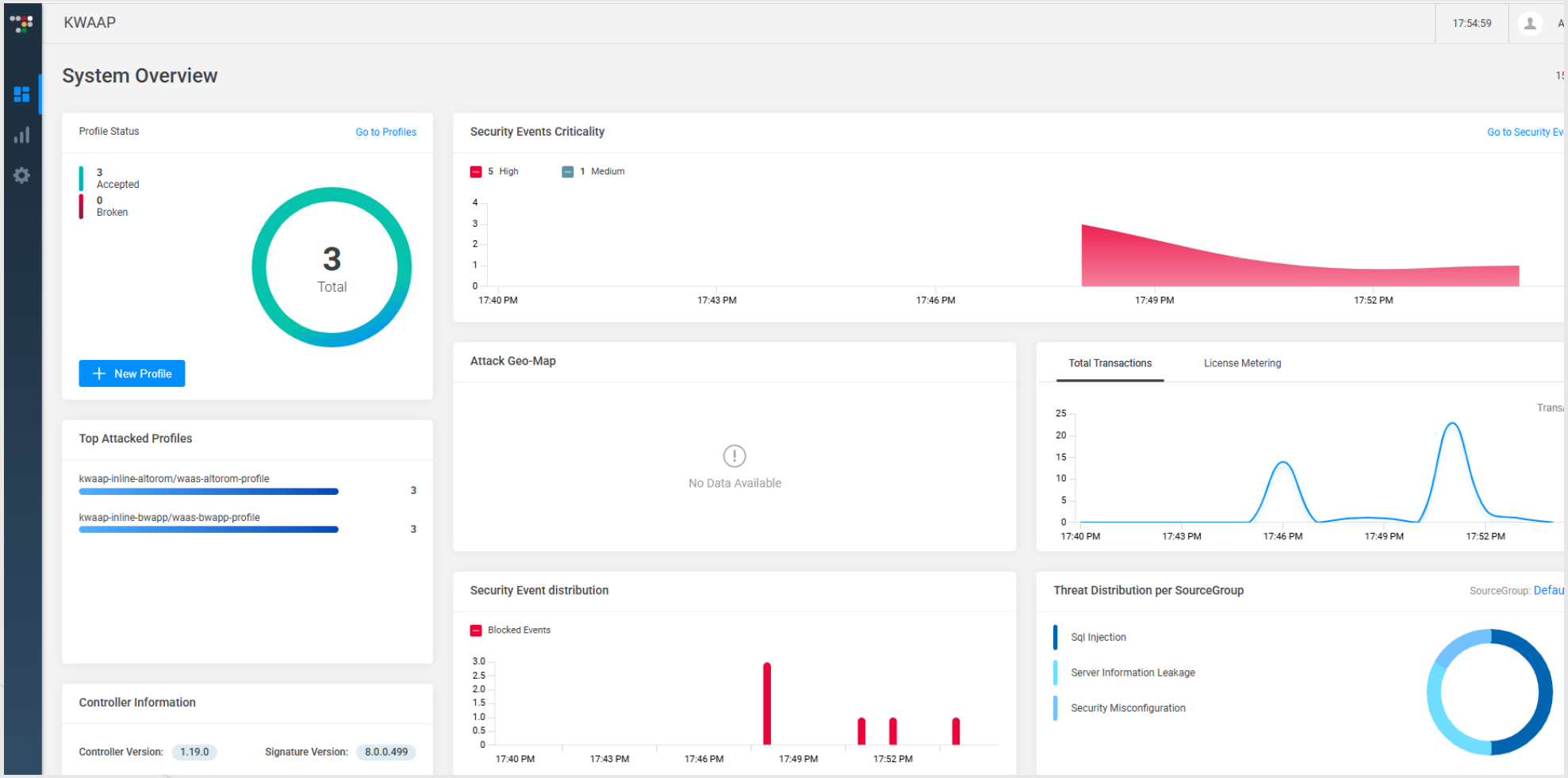


Security Events

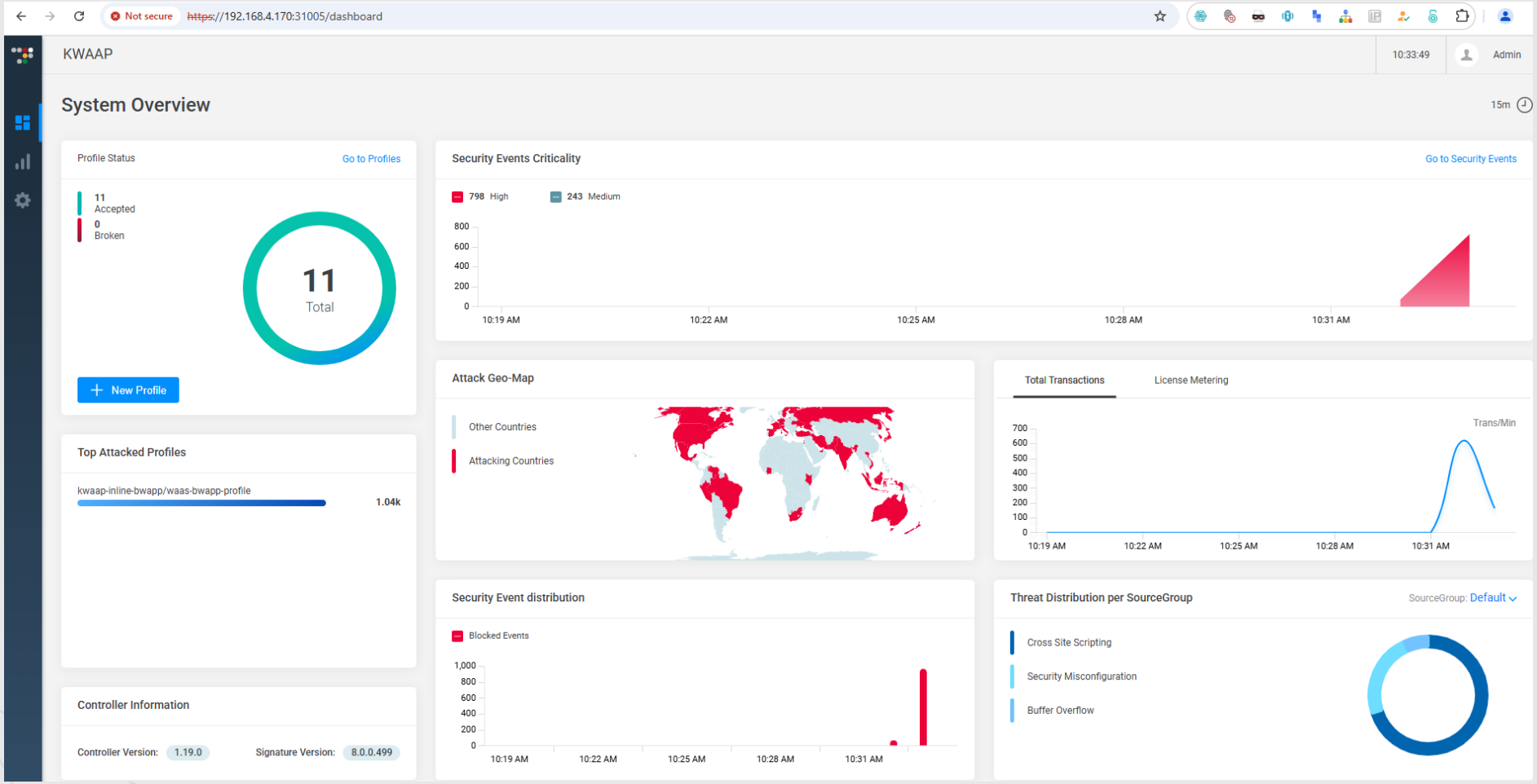
Export Selected | Export All

Action	Time & Date	Severity	Client Source	Location	Hostname	Threat	Attack Name	Module
Blocked	06-02-25 17:52:11		10.42.0.0:45432	N/A	192.168.4.170:31024	Misconfiguration	Security Misconfiguration	Known Attacks - Signature ...
Blocked	06-02-25 17:51:06		10.42.0.0:24559	N/A	192.168.4.170:31024	Data Leakage	Server Information Leakage	Known Attacks - Signature ...
Blocked	06-02-25 17:48:53		10.42.0.0:58608	N/A	192.168.4.170:31021	SQL Threat	SQL Injection	Known Attacks - Expressio...
Blocked	06-02-25 17:48:53		10.42.0.0:58608	N/A	192.168.4.170:31021	Always True manipulations...	SQL Injection	Known Attacks - Expressio...
Blocked	06-02-25 17:48:53		10.42.0.0:58608	N/A	192.168.4.170:31021	Always True manipulations...	SQL Injection	Known Attacks - Expressio...

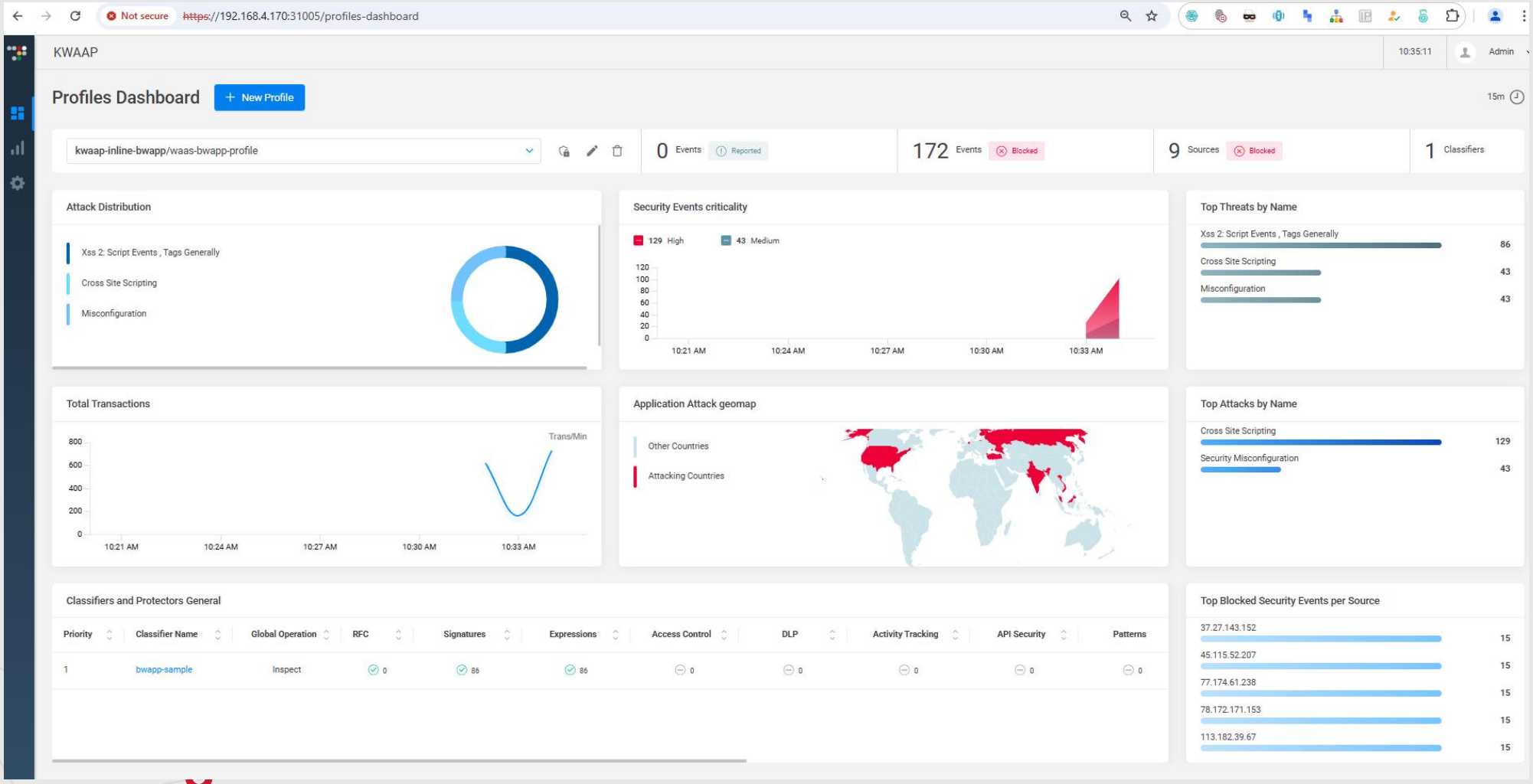
Detection and Reporting



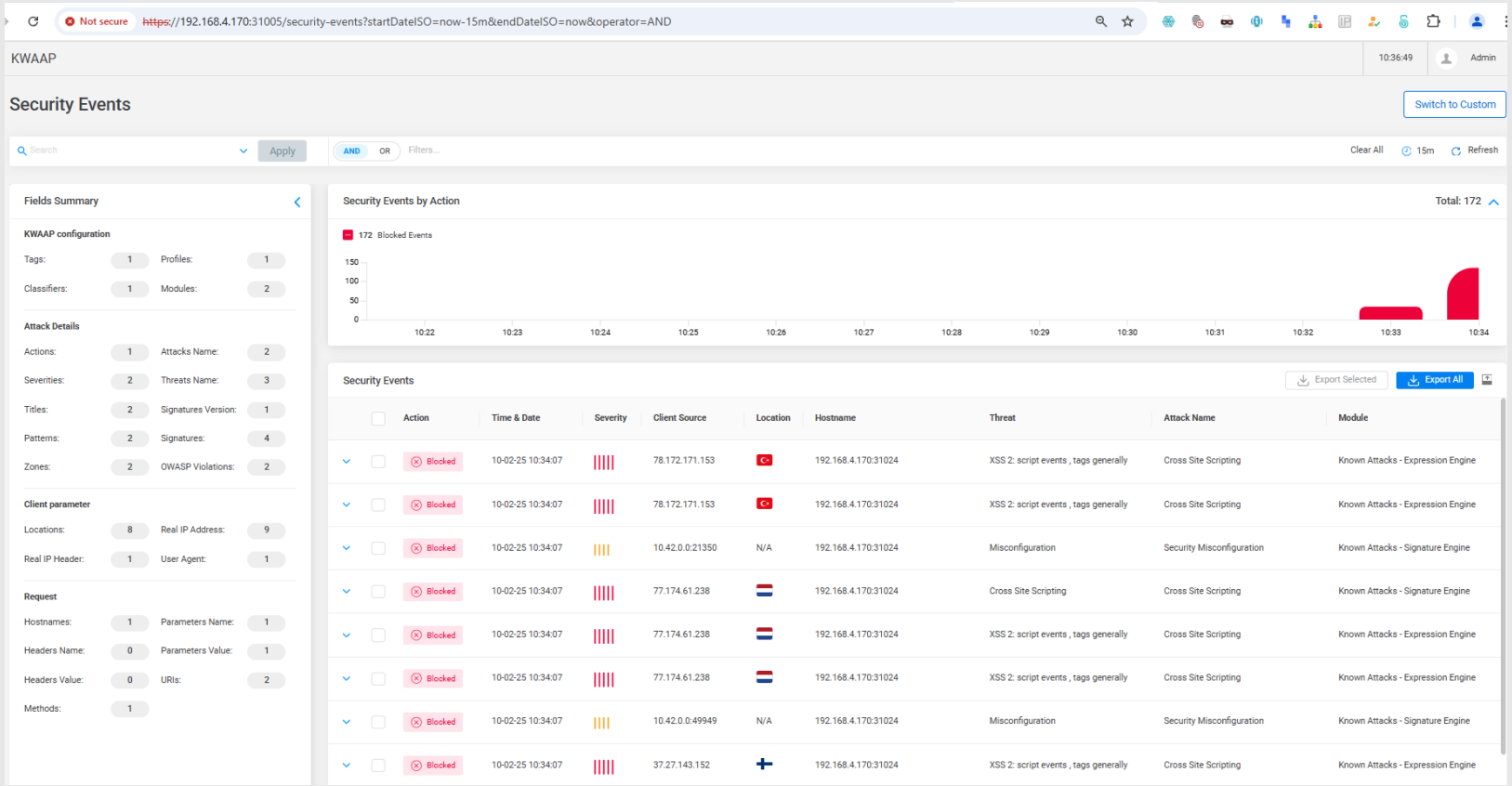
KWAAP Security Dashboard



KWAAP Security Dashboard



KWAAP Security Event Analysis



Radware KWAAP infrastructure Monitoring in NeuVector

Not secure https://192.168.4.170:32689/api/v1/namespaces/cattle-neuvector-system/services/https:neuvector-service-webui:8443/proxy/#/workloads

NeuVector BY SUSE

cluster.local

- Dashboard
- Network Activity
- Assets
  - Platforms
  - Namespaces
  - Nodes
  - Containers
  - Registries
  - Sigstore Verifiers
  - System Components
- Policy
- Security Risks

Containers

Auto Scan | View | Re

Total: 61

Scan | Filter

Name	Namespace	Node	Applications	State	Scan Status	High	Medium	Scanned at
waas-validation-controller-deployment-!	kwaf	suse04172.intrusis.io	SSL,TCP/8080	Discover	Finished	0	0	Feb 06, 2025 17:58:44
validationcontroller	kwaf	suse04172.intrusis.io	TCP/4443,TCP/8080	Discover		0	0	
waas-redis-statefulset-0	kwaf	suse04171.intrusis.io	Redis,TCP/9121	Discover		0	0	
redis	kwaf	suse04171.intrusis.io	Redis	Discover		0	0	
exporter	kwaf	suse04171.intrusis.io	TCP/9121	Discover		0	0	
waas-rate-limiter-deployment-7866d6c6	kwaf	suse04172.intrusis.io	TCP/8081,TCP/8080	Discover		0	0	
rater	kwaf	suse04172.intrusis.io	TCP/8080,TCP/8081	Discover		0	0	
waas-profiles-crud-deployment-786649(	kwaf	suse04171.intrusis.io	HTTP	Discover		0	0	
profiles	kwaf	suse04171.intrusis.io	TCP/8080	Discover		0	0	
waas-logstash-deployment-866875cd95	kwaf	suse04172.intrusis.io	HTTP	Discover		0	0	
logstash	kwaf	suse04172.intrusis.io	TCP/2020,TCP/9600	Discover		0	0	
waas-gui-deployment-69b8d88c5c-9jln9	kwaf	suse04172.intrusis.io	nginx,SSL,TCP/9000	Discover		0	0	
identity	kwaf	suse04172.intrusis.io	TCP/9000	Discover		0	0	
gui	kwaf	suse04172.intrusis.io	nginx	Discover		0	0	
waas-events-fetcher-deployment-5f94fcl	kwaf	suse04171.intrusis.io	HTTP	Discover		0	0	
events-fetcher	kwaf	suse04171.intrusis.io	TCP/8080	Discover		0	0	
waas-elasticsearch-deployment-0	kwaf	suse04172.intrusis.io	ElasticSearch,SSL	Discover		0	0	
elasticsearch	kwaf	suse04172.intrusis.io	ElasticSearch	Discover		0	0	

CIS Benchmark Monitoring

Not secure https://192.168.4.170:32689/dashboard/c/local/cis/cis.cattle.io.clusterscan/scan-s72zk

local

- Cluster
- Workloads
- Apps
- Service Discovery
- Storage
- Policy
- Monitoring
- CIS Benchmark
  - Scans 3
  - Profiles 14
  - Benchmark Versions 14
- NeuVector
- More Resources

Scan: scan-s72zk Fail

Detail | Config

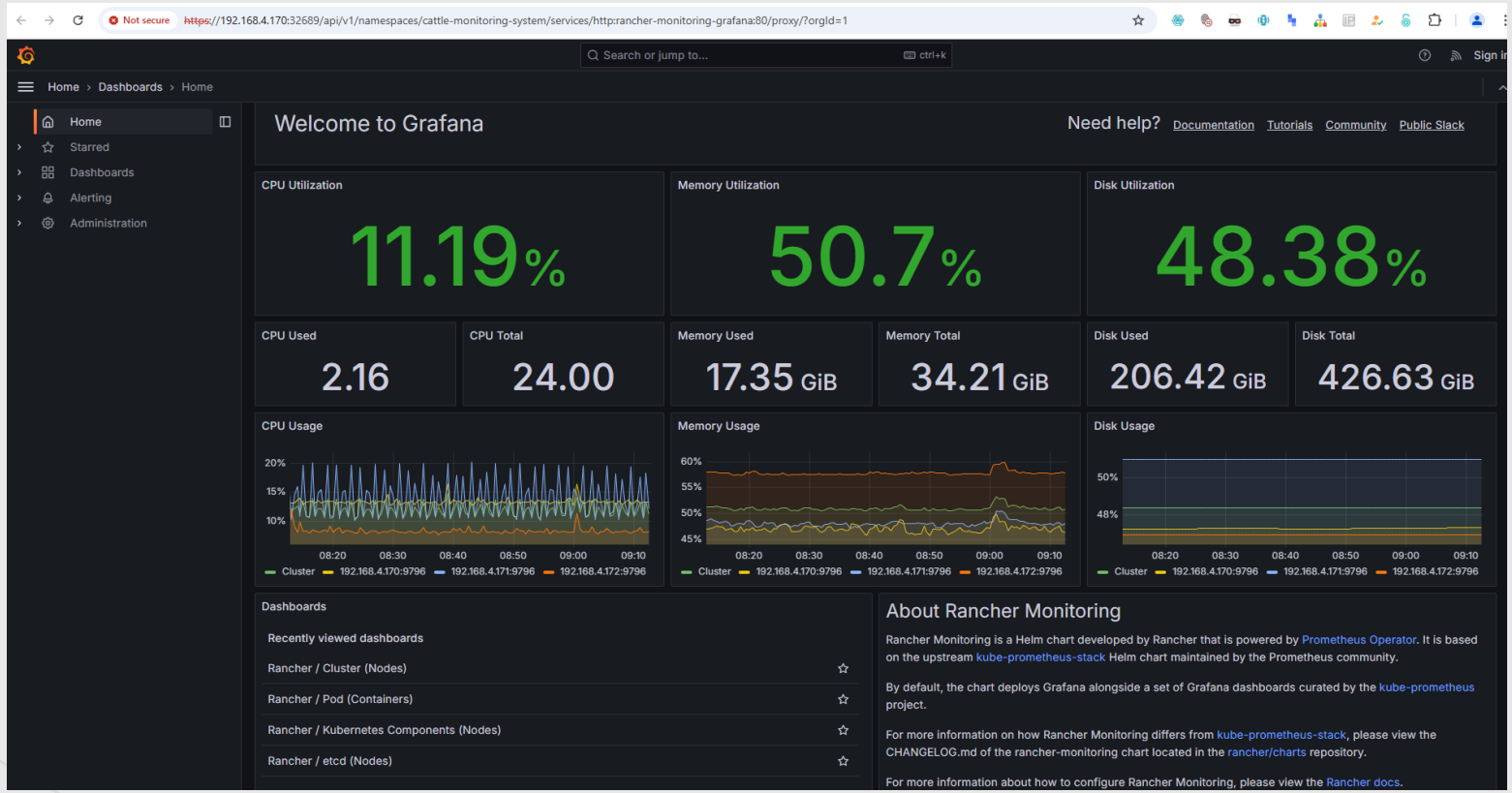
ClusterScan complete, there are some test failures, please check the ClusterScanReport

Profile: rke2-cis-1.9-profile | Total: 130 | Pass: 73 | Warn: 44 | Skip: 0 | Fail: 8 | N/A: 5 | Last Scan Time: Thu, Feb 6 2025 12:43

State	Number	Description
Fail	1.2.16	Ensure that the --audit-log-path argument is set (Automated)
Fail	1.2.17	Ensure that the --audit-log-maxage argument is set to 30 or as appropriate (Automated)
Fail	1.2.18	Ensure that the --audit-log-maxbackup argument is set to 10 or as appropriate (Automated)
Fail	1.2.19	Ensure that the --audit-log-maxsize argument is set to 100 or as appropriate (Automated)
Fail	3.2.1	Ensure that a minimal audit policy is created (Automated)
Fail	5.1.3	Minimize wildcard use in Roles and ClusterRoles (Automated)
Fail	5.1.5	Ensure that default service accounts are not actively used. (Automated)
Fail	5.1.6	Ensure that Service Account Tokens are only mounted where necessary (Automated)
Warn	1.1.7	Ensure that the etcd pod specification file permissions are set to 600 or more restrictive (Manual)
Warn	1.1.9	Ensure that the Container Network Interface file permissions are set to 600 or more restrictive (Manual)
Warn	1.1.12	Ensure that the etcd data directory ownership is set to etcd:etcd (Manual)
Warn	1.1.20	Ensure that the Kubernetes PKI certificate file permissions are set to 600 or more restrictive (Manual)

Grafana Monitoring

- Radware has a number of Grafana Dashboards that can be imported into Rancher



Thank you!

radware