aqua

Integrating Cloud Native Security into the SRE culture

Anais Urlichs

© 2022 Aqua Security Software Ltd., All Rights Reserved

@urlichsanais

Topic

Site Reliability Engineering

Cloud Native Security

Who am I?

Accepted first role in the cloud native space
without knowing what cloud native was
Developer Advocacy
-- this time for open source
Stumbled into Developer Advocacy
Tried to be an SRE
YouTube
CNCF Ambassador of the year
Open Source Blockchain Space
Cloud Native

YouTube

@urlichsanais

Weekly DevOps Newsletter

DevOps

DevOps Diary Weekly Newsletter and DevOps related blog posts

10 OCT 2022
PUBLIC

#69 Seven-Day DevOps — Weekly DevOps Newsletter

Weekly Newsletter with pupdates, tutorials, videos, fun memes and more!

5 OCT 2022
PUBLIC

Writing a microk8s addon on Mac

In this blog post, I first describe the steps I took to install microk8s and then to develop and test a microk8s addon for the Trivy...

22 SEP 2022
PUBLIC

#68 Seven-Day DevOps — Weekly DevOps Newsletter

Some exciting updates, great content incl. tutorials, talks and more events. Enjoy!

8 SEP 2022
PUBLIC

#67 Seven-Day DevOps — Weekly DevOps Newsletter

This week's newsletter is featuring lots of content on AWS, including tutorials, tweet-threads and podcasts – among other excitin...

@urlichsanais

@urlichsanais

Supercluster design: compute

2xIntel Gold Xeon 20 core CPU
384GB 2666Mhz DRAM
100 Gb Networking

OPEN Compute Project®

@urlichsanais

SRE Culture – What is it?

DevSecOps/Cloud Native Security

DevSecOps

Incorporating security into all other business functions
by empowering people and creating accountability

The premise

Healthy Services are Secure Services

↑

Define what healthy services look like

SRE Goals are Security Goals

aqua

Practices

- Investing in runbooks and documentation
- Developing a robust delivery pipeline
- Define ownership
- Set explicit expectations on people
- Active communication with engineers
- Define procedures/processes
- Define use and expectations on tools

Tools

Observability

Management

CI/CD

aqua

Where are the security tools?

10 Steps to integrating cloud native security

Scan Targets

- Git Repository & Filesystem Scanning
- Container Image Scanning
- Dockerfile Scanning
- IaC Scanning
- Kubernetes Manifest Scanning
- SBOM Generation & Scanning
- AWS Account Scanning
- In-cluster Scanning

aqua

Step 1 Understanding your need

Factors

- Size of your team
- Industry you are working in
- Type of technologies you are working with
- Company Goals and leadership
- Budget and expertise

aqua

INSTALLATION

KUBERNETES RESOURCE TYPE

SCAN COVERAGE

INTEGRATION

FOCUS

@urlichsanais

Needs – Based on Wise Engineering Blog post

1. Assign ownership of vulnerabilities
2. Global view of the security state of services
3. Develop Dashboards for different users and requirements
4. Overcome difficult to use different UIs

Note that these needs have been rewritten based on the following blog post https://medium.com/wise-engineering/our-application-security-journey-part-1-fb7d449a7126

Step 2 Choosing a cloud native Security Scanner

Open Source Security Scanning -- focus on cloud native

Vulnerability Scans

- Trivy
- Clair
- Grype
- KubeClarity

IaC Misconfiguration Scans

- Trivy
- tfsec
- terrascan
- KICS
- checkov
- Conftest
- Kubescape
- regula

Policy Checks & Schema validation*

- Trivy
- CloudQuery
- Cloud Custodian

*a little vague since multiple tools that implement Rego etc. allow for policy checks

Compliance Scans

- kube-bench CIS
- kube-beacon CIS
- chain-bench CIS
- Starboard NSA
- Kubescape NSA

SBOM

- Trivy
- Syft
- CloudQuery
- KubeClarity

In-Cluster Scans

- Trivy
- Kubescape

Kubernetes Pentesting

- kube-hunter
- kdigger
- StackRox

Secret Scanning

- tfsec (terraform)
- Trivy (K8s)

many-more non cloud native

@urlichsanais

Scan Targets

- Git Repository & Filesystem Scanning
- Container Image Scanning
- Dockerfile Scanning
- IaC Scanning
- Kubernetes Manifest Scanning
- SBOM Generation & Scanning
- AWS Account Scanning
- In-cluster Scanning

aqua

Step 3 Setting it up & Making sure everything is running properly

1. Identifying the best installation option
2. Deciding upon the configuration
3. Testing custom configuration
4. Ensuring everything is working together

HELM

@urlichsanais

Kubernetes Cluster
app namespace
App
monitoring namespace
Prometheus
Grafana
trivy-system ns
Trivy Operator

aqua

If everything is a Kubernetes resource, you can use the same processes across your stack

```
❯ kubectl get all -n trivy-system
NAME                                  READY   STATUS    RESTARTS   AGE
pod/trivy-operator-8556cdf857-snhdj   1/1     Running   0          4m56s

NAME                     TYPE        CLUSTER-IP   EXTERNAL-IP   PORT(S)   AGE
service/trivy-operator   ClusterIP   None         <none>        80/TCP    4m56s

NAME                             READY   UP-TO-DATE   AVAILABLE   AGE
deployment.apps/trivy-operator   1/1     1            1           4m57s

NAME                                        DESIRED   CURRENT   READY   AGE
replicaset.apps/trivy-operator-8556cdf857   1         1         1       4m57s
  return go(f, seed, [])
}
```

```
trivy_image_vulnerabilities{image_digest="",image_registry="index.docker.io",image_repository="grafana/grafana",image_tag="9.1.6",name="replicaset-prom-grafana-54894696b-grafana",namespace="monitoring",severity="Critical"} 0
trivy_image_vulnerabilities{image_digest="",image_registry="index.docker.io",image_repository="grafana/grafana",image_tag="9.1.6",name="replicaset-prom-grafana-54894696b-grafana",namespace="monitoring",severity="High"} 2
trivy_image_vulnerabilities{image_digest="",image_registry="index.docker.io",image_repository="grafana/grafana",image_tag="9.1.6",name="replicaset-prom-grafana-54894696b-grafana",namespace="monitoring",severity="Low"} 0
trivy_image_vulnerabilities{image_digest="",image_registry="index.docker.io",image_repository="grafana/grafana",image_tag="9.1.6",name="replicaset-prom-grafana-54894696b-grafana",namespace="monitoring",severity="Medium"} 2
trivy_image_vulnerabilities{image_digest="",image_registry="index.docker.io",image_repository="grafana/grafana",image_tag="9.1.6",name="replicaset-prom-grafana-54894696b-grafana",namespace="monitoring",severity="Unknown"} 0
trivy_image_vulnerabilities{image_digest="",image_registry="index.docker.io",image_repository="grafana/loki",image_tag="2.6.1",name="replicaset-74b7d79776",namespace="monitoring",severity="Critical"} 1
trivy_image_vulnerabilities{image_digest="",image_registry="index.docker.io",image_repository="grafana/loki",image_tag="2.6.1",name="replicaset-74b7d79776",namespace="monitoring",severity="High"} 2
trivy_image_vulnerabilities{image_digest="",image_registry="index.docker.io",image_repository="grafana/loki",image_tag="2.6.1",name="replicaset-74b7d79776",namespace="monitoring",severity="Low"} 0
trivy_image_vulnerabilities{image_digest="",image_registry="index.docker.io",image_repository="grafana/loki",image_tag="2.6.1",name="replicaset-74b7d79776",namespace="monitoring",severity="Medium"} 4
trivy_image_vulnerabilities{image_digest="",image_registry="index.docker.io",image_repository="grafana/loki",image_tag="2.6.1",name="replicaset-74b7d79776",namespace="monitoring",severity="Unknown"} 1
trivy_image_vulnerabilities{image_digest="",image_registry="index.docker.io",image_repository="grafana/loki",image_tag="2.6.1",name="replicaset-785b7655f",namespace="monitoring",severity="Critical"} 1
trivy_image_vulnerabilities{image_digest="",image_registry="index.docker.io",image_repository="grafana/loki",image_tag="2.6.1",name="replicaset-785b7655f",namespace="monitoring",severity="High"} 2
trivy_image_vulnerabilities{image_digest="",image_registry="index.docker.io",image_repository="grafana/loki",image_tag="2.6.1",name="replicaset-785b7655f",namespace="monitoring",severity="Low"} 0
trivy_image_vulnerabilities{image_digest="",image_registry="index.docker.io",image_repository="grafana/loki",image_tag="2.6.1",name="replicaset-785b7655f",namespace="monitoring",severity="Medium"} 4
trivy_image_vulnerabilities{image_digest="",image_registry="index.docker.io",image_repository="grafana/loki",image_tag="2.6.1",name="replicaset-785b7655f",namespace="monitoring",severity="Unknown"} 1
trivy_image_vulnerabilities{image_digest="",image_registry="index.docker.io",image_repository="grafana/loki",image_tag="2.6.1",name="statefulset-loki-loki-distributed-ingester-ingester",namespace="monitoring",severity="Critical"} 1
trivy_image_vulnerabilities{image_digest="",image_registry="index.docker.io",image_repository="grafana/loki",image_tag="2.6.1",name="statefulset-loki-loki-distributed-ingester-ingester",namespace="monitoring",severity="High"} 2
trivy_image_vulnerabilities{image_digest="",image_registry="index.docker.io",image_repository="grafana/loki",image_tag="2.6.1",name="statefulset-loki-loki-distributed-ingester-ingester",namespace="monitoring",severity="Low"} 0
trivy_image_vulnerabilities{image_digest="",image_registry="index.docker.io",image_repository="grafana/loki",image_tag="2.6.1",name="statefulset-loki-loki-distributed-ingester-ingester",namespace="monitoring",severity="Medium"} 4
trivy_image_vulnerabilities{image_digest="",image_registry="index.docker.io",image_repository="grafana/loki",image_tag="2.6.1",name="statefulset-loki-loki-distributed-ingester-ingester",namespace="monitoring",severity="Unknown"} 1
trivy_image_vulnerabilities{image_digest="",image_registry="index.docker.io",image_repository="grafana/loki",image_tag="2.6.1",name="statefulset-loki-loki-distributed-querier-querier",namespace="monitoring",severity="Critical"} 1
trivy_image_vulnerabilities{image_digest="",image_registry="index.docker.io",image_repository="grafana/loki",image_tag="2.6.1",name="statefulset-loki-loki-distributed-querier-querier",namespace="monitoring",severity="High"} 2
trivy_image_vulnerabilities{image_digest="",image_registry="index.docker.io",image_repository="grafana/loki",image_tag="2.6.1",name="statefulset-loki-loki-distributed-querier-querier",namespace="monitoring",severity="Low"} 0
trivy_image_vulnerabilities{image_digest="",image_registry="index.docker.io",image_repository="grafana/loki",image_tag="2.6.1",name="statefulset-loki-loki-distributed-querier-querier",namespace="monitoring",severity="Medium"} 4
trivy_image_vulnerabilities{image_digest="",image_registry="index.docker.io",image_repository="grafana/loki",image_tag="2.6.1",name="statefulset-loki-loki-distributed-querier-querier",namespace="monitoring",severity="Unknown"} 1
trivy_image_vulnerabilities{image_digest="",image_registry="index.docker.io",image_repository="nginxinc/nginx-unprivileged",image_tag="1.19-alpine",name="replicaset-loki-loki-distributed-gateway-6595fd6d55-nginx",namespace="monitoring",severity="Critical"} 9
trivy_image_vulnerabilities{image_digest="",image_registry="index.docker.io",image_repository="nginxinc/nginx-unprivileged",image_tag="1.19-alpine",name="replicaset-loki-loki-distributed-gateway-6595fd6d55-nginx",namespace="monitoring",severity="High"} 50
trivy_image_vulnerabilities{image_digest="",image_registry="index.docker.io",image_repository="nginxinc/nginx-unprivileged",image_tag="1.19-alpine",name="replicaset-loki-loki-distributed-gateway-6595fd6d55-nginx",namespace="monitoring",severity="Low"} 6
trivy_image_vulnerabilities{image_digest="",image_registry="index.docker.io",image_repository="nginxinc/nginx-unprivileged",image_tag="1.19-alpine",name="replicaset-loki-loki-distributed-gateway-6595fd6d55-nginx",namespace="monitoring",severity="Medium"} 29
trivy_image_vulnerabilities{image_digest="",image_registry="index.docker.io",image_repository="nginxinc/nginx-unprivileged",image_tag="1.19-alpine",name="replicaset-loki-loki-distributed-gateway-6595fd6d55-nginx",namespace="monitoring",severity="Unknown"} 0
trivy_image_vulnerabilities{image_digest="",image_registry="quay.io",image_repository="kiwigrid/k8s-sidecar",image_tag="1.19.2",name="replicaset-prom-grafana-54894696b-grafana-sc-dashboard",namespace="monitoring",severity="Critical"} 2
trivy_image_vulnerabilities{image_digest="",image_registry="quay.io",image_repository="kiwigrid/k8s-sidecar",image_tag="1.19.2",name="replicaset-prom-grafana-54894696b-grafana-sc-dashboard",namespace="monitoring",severity="High"} 4
trivy_image_vulnerabilities{image_digest="",image_registry="quay.io",image_repository="kiwigrid/k8s-sidecar",image_tag="1.19.2",name="replicaset-prom-grafana-54894696b-grafana-sc-dashboard",namespace="monitoring",severity="Low"} 0
trivy_image_vulnerabilities{image_digest="",image_registry="quay.io",image_repository="kiwigrid/k8s-sidecar",image_tag="1.19.2",name="replicaset-prom-grafana-54894696b-grafana-sc-dashboard",namespace="monitoring",severity="Medium"} 3
trivy_image_vulnerabilities{image_digest="",image_registry="quay.io",image_repository="kiwigrid/k8s-sidecar",image_tag="1.19.2",name="replicaset-prom-grafana-54894696b-grafana-sc-dashboard",namespace="monitoring",severity="Unknown"} 0
trivy_image_vulnerabilities{image_digest="",image_registry="quay.io",image_repository="kiwigrid/k8s-sidecar",image_tag="1.19.2",name="replicaset-prom-grafana-54894696b-grafana-sc-datasources",namespace="monitoring",severity="Critical"} 2
trivy_image_vulnerabilities{image_digest="",image_registry="quay.io",image_repository="kiwigrid/k8s-sidecar",image_tag="1.19.2",name="replicaset-prom-grafana-54894696b-grafana-sc-datasources",namespace="monitoring",severity="High"} 4
trivy_image_vulnerabilities{image_digest="",image_registry="quay.io",image_repository="kiwigrid/k8s-sidecar",image_tag="1.19.2",name="replicaset-prom-grafana-54894696b-grafana-sc-datasources",namespace="monitoring",severity="Low"} 0
trivy_image_vulnerabilities{image_digest="",image_registry="quay.io",image_repository="kiwigrid/k8s-sidecar",image_tag="1.19.2",name="replicaset-prom-grafana-54894696b-grafana-sc-datasources",namespace="monitoring",severity="Medium"} 3
trivy_image_vulnerabilities{image_digest="",image_registry="quay.io",image_repository="kiwigrid/k8s-sidecar",image_tag="1.19.2",name="replicaset-prom-grafana-54894696b-grafana-sc-datasources",namespace="monitoring",severity="Unknown"} 0
trivy_image_vulnerabilities{image_digest="",image_registry="quay.io",image_repository="prometheus-operator/prometheus-config-reloader",image_tag="v0.59.2",name="statefulset-6cdd4b9bbc",namespace="monitoring",severity="Critical"} 0
trivy_image_vulnerabilities{image_digest="",image_registry="quay.io",image_repository="prometheus-operator/prometheus-config-reloader",image_tag="v0.59.2",name="statefulset-6cdd4b9bbc",namespace="monitoring",severity="High"} 0
trivy_image_vulnerabilities{image_digest="",image_registry="quay.io",image_repository="prometheus-operator/prometheus-config-reloader",image_tag="v0.59.2",name="statefulset-6cdd4b9bbc",namespace="monitoring",severity="Low"} 0
trivy_image_vulnerabilities{image_digest="",image_registry="quay.io",image_repository="prometheus-operator/prometheus-config-reloader",image_tag="v0.59.2",name="statefulset-6cdd4b9bbc",namespace="monitoring",severity="Medium"} 0
trivy_image_vulnerabilities{image_digest="",image_registry="quay.io",image_repository="prometheus-operator/prometheus-config-reloader",image_tag="v0.59.2",name="statefulset-6cdd4b9bbc",namespace="monitoring",severity="Unknown"} 0
trivy_image_vulnerabilities{image_digest="",image_registry="quay.io",image_repository="prometheus-operator/prometheus-operator",image_tag="v0.59.2",name="replicaset-64fbf79f9c",namespace="monitoring",severity="Critical"} 0
trivy_image_vulnerabilities{image_digest="",image_registry="quay.io",image_repository="prometheus-operator/prometheus-operator",image_tag="v0.59.2",name="replicaset-64fbf79f9c",namespace="monitoring",severity="High"} 1
trivy_image_vulnerabilities{image_digest="",image_registry="quay.io",image_repository="prometheus-operator/prometheus-operator",image_tag="v0.59.2",name="replicaset-64fbf79f9c",namespace="monitoring",severity="Low"} 0
trivy_image_vulnerabilities{image_digest="",image_registry="quay.io",image_repository="prometheus-operator/prometheus-operator",image_tag="v0.59.2",name="replicaset-64fbf79f9c",namespace="monitoring",severity="Medium"} 1
trivy_image_vulnerabilities{image_digest="",image_registry="quay.io",image_repository="prometheus-operator/prometheus-operator",image_tag="v0.59.2",name="replicaset-64fbf79f9c",namespace="monitoring",severity="Unknown"} 0
trivy_image_vulnerabilities{image_digest="",image_registry="quay.io",image_repository="prometheus/alertmanager",image_tag="v0.24.0",name="statefulset-85b74b95b5",namespace="monitoring",severity="Critical"} 0
trivy_image_vulnerabilities{image_digest="",image_registry="quay.io",image_repository="prometheus/alertmanager",image_tag="v0.24.0",name="statefulset-85b74b95b5",namespace="monitoring",severity="High"} 6
trivy_image_vulnerabilities{image_digest="",image_registry="quay.io",image_repository="prometheus/alertmanager",image_tag="v0.24.0",name="statefulset-85b74b95b5",namespace="monitoring",severity="Low"} 0
trivy_image_vulnerabilities{image_digest="",image_registry="quay.io",image_repository="prometheus/alertmanager",image_tag="v0.24.0",name="statefulset-85b74b95b5",namespace="monitoring",severity="Medium"} 2
trivy_image_vulnerabilities{image_digest="",image_registry="quay.io",image_repository="prometheus/alertmanager",image_tag="v0.24.0",name="statefulset-85b74b95b5",namespace="monitoring",severity="Unknown"} 4
```

```
trivy_image_exposedsecrets{image_digest="",image_registry="index.docker.io",image_repository="grafana/grafana",image_tag="9.1.6",name="replicaset-prom-grafana-54894696b-grafana",namespace="monitoring",severity="Critical"} 0
trivy_image_exposedsecrets{image_digest="",image_registry="index.docker.io",image_repository="grafana/grafana",image_tag="9.1.6",name="replicaset-prom-grafana-54894696b-grafana",namespace="monitoring",severity="High"} 0
trivy_image_exposedsecrets{image_digest="",image_registry="index.docker.io",image_repository="grafana/grafana",image_tag="9.1.6",name="replicaset-prom-grafana-54894696b-grafana",namespace="monitoring",severity="Low"} 0
trivy_image_exposedsecrets{image_digest="",image_registry="index.docker.io",image_repository="grafana/grafana",image_tag="9.1.6",name="replicaset-prom-grafana-54894696b-grafana",namespace="monitoring",severity="Medium"} 0
trivy_image_exposedsecrets{image_digest="",image_registry="index.docker.io",image_repository="grafana/loki",image_tag="2.6.1",name="replicaset-74b7d79776",namespace="monitoring",severity="Critical"} 0
trivy_image_exposedsecrets{image_digest="",image_registry="index.docker.io",image_repository="grafana/loki",image_tag="2.6.1",name="replicaset-74b7d79776",namespace="monitoring",severity="High"} 0
trivy_image_exposedsecrets{image_digest="",image_registry="index.docker.io",image_repository="grafana/loki",image_tag="2.6.1",name="replicaset-74b7d79776",namespace="monitoring",severity="Low"} 0
trivy_image_exposedsecrets{image_digest="",image_registry="index.docker.io",image_repository="grafana/loki",image_tag="2.6.1",name="replicaset-74b7d79776",namespace="monitoring",severity="Medium"} 0
trivy_image_exposedsecrets{image_digest="",image_registry="index.docker.io",image_repository="grafana/loki",image_tag="2.6.1",name="replicaset-785b7655f",namespace="monitoring",severity="Critical"} 0
trivy_image_exposedsecrets{image_digest="",image_registry="index.docker.io",image_repository="grafana/loki",image_tag="2.6.1",name="replicaset-785b7655f",namespace="monitoring",severity="High"} 0
trivy_image_exposedsecrets{image_digest="",image_registry="index.docker.io",image_repository="grafana/loki",image_tag="2.6.1",name="replicaset-785b7655f",namespace="monitoring",severity="Low"} 0
trivy_image_exposedsecrets{image_digest="",image_registry="index.docker.io",image_repository="grafana/loki",image_tag="2.6.1",name="replicaset-785b7655f",namespace="monitoring",severity="Medium"} 0
trivy_image_exposedsecrets{image_digest="",image_registry="index.docker.io",image_repository="grafana/loki",image_tag="2.6.1",name="statefulset-loki-loki-distributed-ingester-ingester",namespace="monitoring",severity="Critical"} 0
trivy_image_exposedsecrets{image_digest="",image_registry="index.docker.io",image_repository="grafana/loki",image_tag="2.6.1",name="statefulset-loki-loki-distributed-ingester-ingester",namespace="monitoring",severity="High"} 0
trivy_image_exposedsecrets{image_digest="",image_registry="index.docker.io",image_repository="grafana/loki",image_tag="2.6.1",name="statefulset-loki-loki-distributed-ingester-ingester",namespace="monitoring",severity="Low"} 0
trivy_image_exposedsecrets{image_digest="",image_registry="index.docker.io",image_repository="grafana/loki",image_tag="2.6.1",name="statefulset-loki-loki-distributed-ingester-ingester",namespace="monitoring",severity="Medium"} 0
trivy_image_exposedsecrets{image_digest="",image_registry="index.docker.io",image_repository="grafana/loki",image_tag="2.6.1",name="statefulset-loki-loki-distributed-querier-querier",namespace="monitoring",severity="Critical"} 0
trivy_image_exposedsecrets{image_digest="",image_registry="index.docker.io",image_repository="grafana/loki",image_tag="2.6.1",name="statefulset-loki-loki-distributed-querier-querier",namespace="monitoring",severity="High"} 0
trivy_image_exposedsecrets{image_digest="",image_registry="index.docker.io",image_repository="grafana/loki",image_tag="2.6.1",name="statefulset-loki-loki-distributed-querier-querier",namespace="monitoring",severity="Low"} 0
trivy_image_exposedsecrets{image_digest="",image_registry="index.docker.io",image_repository="grafana/loki",image_tag="2.6.1",name="statefulset-loki-loki-distributed-querier-querier",namespace="monitoring",severity="Medium"} 0
trivy_image_exposedsecrets{image_digest="",image_registry="index.docker.io",image_repository="nginxinc/nginx-unprivileged",image_tag="1.19-alpine",name="replicaset-loki-loki-distributed-gateway-6595fd6d55-nginx",namespace="monitoring",severity="Critical"} 0
trivy_image_exposedsecrets{image_digest="",image_registry="index.docker.io",image_repository="nginxinc/nginx-unprivileged",image_tag="1.19-alpine",name="replicaset-loki-loki-distributed-gateway-6595fd6d55-nginx",namespace="monitoring",severity="High"} 0
trivy_image_exposedsecrets{image_digest="",image_registry="index.docker.io",image_repository="nginxinc/nginx-unprivileged",image_tag="1.19-alpine",name="replicaset-loki-loki-distributed-gateway-6595fd6d55-nginx",namespace="monitoring",severity="Low"} 0
trivy_image_exposedsecrets{image_digest="",image_registry="index.docker.io",image_repository="nginxinc/nginx-unprivileged",image_tag="1.19-alpine",name="replicaset-loki-loki-distributed-gateway-6595fd6d55-nginx",namespace="monitoring",severity="Medium"} 0
trivy_image_exposedsecrets{image_digest="",image_registry="quay.io",image_repository="kiwigrid/k8s-sidecar",image_tag="1.19.2",name="replicaset-prom-grafana-54894696b-grafana-sc-dashboard",namespace="monitoring",severity="Critical"} 0
trivy_image_exposedsecrets{image_digest="",image_registry="quay.io",image_repository="kiwigrid/k8s-sidecar",image_tag="1.19.2",name="replicaset-prom-grafana-54894696b-grafana-sc-dashboard",namespace="monitoring",severity="High"} 0
trivy_image_exposedsecrets{image_digest="",image_registry="quay.io",image_repository="kiwigrid/k8s-sidecar",image_tag="1.19.2",name="replicaset-prom-grafana-54894696b-grafana-sc-dashboard",namespace="monitoring",severity="Low"} 0
trivy_image_exposedsecrets{image_digest="",image_registry="quay.io",image_repository="kiwigrid/k8s-sidecar",image_tag="1.19.2",name="replicaset-prom-grafana-54894696b-grafana-sc-dashboard",namespace="monitoring",severity="Medium"} 0
trivy_image_exposedsecrets{image_digest="",image_registry="quay.io",image_repository="kiwigrid/k8s-sidecar",image_tag="1.19.2",name="replicaset-prom-grafana-54894696b-grafana-sc-datasources",namespace="monitoring",severity="Critical"} 0
trivy_image_exposedsecrets{image_digest="",image_registry="quay.io",image_repository="kiwigrid/k8s-sidecar",image_tag="1.19.2",name="replicaset-prom-grafana-54894696b-grafana-sc-datasources",namespace="monitoring",severity="High"} 0
trivy_image_exposedsecrets{image_digest="",image_registry="quay.io",image_repository="kiwigrid/k8s-sidecar",image_tag="1.19.2",name="replicaset-prom-grafana-54894696b-grafana-sc-datasources",namespace="monitoring",severity="Low"} 0
trivy_image_exposedsecrets{image_digest="",image_registry="quay.io",image_repository="kiwigrid/k8s-sidecar",image_tag="1.19.2",name="replicaset-prom-grafana-54894696b-grafana-sc-datasources",namespace="monitoring",severity="Medium"} 0
trivy_image_exposedsecrets{image_digest="",image_registry="quay.io",image_repository="prometheus-operator/prometheus-config-reloader",image_tag="v0.59.2",name="statefulset-6cdd4b9bbc",namespace="monitoring",severity="Critical"} 0
trivy_image_exposedsecrets{image_digest="",image_registry="quay.io",image_repository="prometheus-operator/prometheus-config-reloader",image_tag="v0.59.2",name="statefulset-6cdd4b9bbc",namespace="monitoring",severity="High"} 0
trivy_image_exposedsecrets{image_digest="",image_registry="quay.io",image_repository="prometheus-operator/prometheus-config-reloader",image_tag="v0.59.2",name="statefulset-6cdd4b9bbc",namespace="monitoring",severity="Low"} 0
trivy_image_exposedsecrets{image_digest="",image_registry="quay.io",image_repository="prometheus-operator/prometheus-config-reloader",image_tag="v0.59.2",name="statefulset-6cdd4b9bbc",namespace="monitoring",severity="Medium"} 0
trivy_image_exposedsecrets{image_digest="",image_registry="quay.io",image_repository="prometheus-operator/prometheus-operator",image_tag="v0.59.2",name="replicaset-64fbf79f9c",namespace="monitoring",severity="Critical"} 0
trivy_image_exposedsecrets{image_digest="",image_registry="quay.io",image_repository="prometheus-operator/prometheus-operator",image_tag="v0.59.2",name="replicaset-64fbf79f9c",namespace="monitoring",severity="High"} 0
trivy_image_exposedsecrets{image_digest="",image_registry="quay.io",image_repository="prometheus-operator/prometheus-operator",image_tag="v0.59.2",name="replicaset-64fbf79f9c",namespace="monitoring",severity="Low"} 0
trivy_image_exposedsecrets{image_digest="",image_registry="quay.io",image_repository="prometheus-operator/prometheus-operator",image_tag="v0.59.2",name="replicaset-64fbf79f9c",namespace="monitoring",severity="Medium"} 0
trivy_image_exposedsecrets{image_digest="",image_registry="quay.io",image_repository="prometheus/alertmanager",image_tag="v0.24.0",name="statefulset-85b74b95b5",namespace="monitoring",severity="Critical"} 0
trivy_image_exposedsecrets{image_digest="",image_registry="quay.io",image_repository="prometheus/alertmanager",image_tag="v0.24.0",name="statefulset-85b74b95b5",namespace="monitoring",severity="High"} 0
trivy_image_exposedsecrets{image_digest="",image_registry="quay.io",image_repository="prometheus/alertmanager",image_tag="v0.24.0",name="statefulset-85b74b95b5",namespace="monitoring",severity="Low"} 0
trivy_image_exposedsecrets{image_digest="",image_registry="quay.io",image_repository="prometheus/alertmanager",image_tag="v0.24.0",name="statefulset-85b74b95b5",namespace="monitoring",severity="Medium"} 0
trivy_image_exposedsecrets{image_digest="",image_registry="quay.io",image_repository="prometheus/node-exporter",image_tag="v1.3.1",name="daemonset-prom-prometheus-node-exporter-node-exporter",namespace="monitoring",severity="Critical"} 0
trivy_image_exposedsecrets{image_digest="",image_registry="quay.io",image_repository="prometheus/node-exporter",image_tag="v1.3.1",name="daemonset-prom-prometheus-node-exporter-node-exporter",namespace="monitoring",severity="High"} 0
trivy_image_exposedsecrets{image_digest="",image_registry="quay.io",image_repository="prometheus/node-exporter",image_tag="v1.3.1",name="daemonset-prom-prometheus-node-exporter-node-exporter",namespace="monitoring",severity="Low"} 0
trivy_image_exposedsecrets{image_digest="",image_registry="quay.io",image_repository="prometheus/node-exporter",image_tag="v1.3.1",name="daemonset-prom-prometheus-node-exporter-node-exporter",namespace="monitoring",severity="Medium"} 0
trivy_image_exposedsecrets{image_digest="",image_registry="registry.k8s.io",image_repository="kube-state-metrics/kube-state-metrics",image_tag="v2.6.0",name="replicaset-84ff6ddf55",namespace="monitoring",severity="Critical"} 0
trivy_image_exposedsecrets{image_digest="",image_registry="registry.k8s.io",image_repository="kube-state-metrics/kube-state-metrics",image_tag="v2.6.0",name="replicaset-84ff6ddf55",namespace="monitoring",severity="High"} 0
trivy_image_exposedsecrets{image_digest="",image_registry="registry.k8s.io",image_repository="kube-state-metrics/kube-state-metrics",image_tag="v2.6.0",name="replicaset-84ff6ddf55",namespace="monitoring",severity="Low"} 0
trivy_image_exposedsecrets{image_digest="",image_registry="registry.k8s.io",image_repository="kube-state-metrics/kube-state-metrics",image_tag="v2.6.0",name="replicaset-84ff6ddf55",namespace="monitoring",severity="Medium"} 0
```

```
trivy_clusterrole_clusterrbacassessments{name="clusterrole-76c6b6cf99",severity="Low"} 0
trivy_clusterrole_clusterrbacassessments{name="clusterrole-76c6b6cf99",severity="Medium"} 0
trivy_clusterrole_clusterrbacassessments{name="clusterrole-77898f44f5",severity="Critical"} 0
trivy_clusterrole_clusterrbacassessments{name="clusterrole-77898f44f5",severity="High"} 1
trivy_clusterrole_clusterrbacassessments{name="clusterrole-77898f44f5",severity="Low"} 0
trivy_clusterrole_clusterrbacassessments{name="clusterrole-77898f44f5",severity="Medium"} 0
trivy_clusterrole_clusterrbacassessments{name="clusterrole-779895897b",severity="Critical"} 0
trivy_clusterrole_clusterrbacassessments{name="clusterrole-779895897b",severity="High"} 0
trivy_clusterrole_clusterrbacassessments{name="clusterrole-779895897b",severity="Low"} 0
trivy_clusterrole_clusterrbacassessments{name="clusterrole-779895897b",severity="Medium"} 0
trivy_clusterrole_clusterrbacassessments{name="clusterrole-779f88d9b5",severity="Critical"} 0
trivy_clusterrole_clusterrbacassessments{name="clusterrole-779f88d9b5",severity="High"} 1
trivy_clusterrole_clusterrbacassessments{name="clusterrole-779f88d9b5",severity="Low"} 0
trivy_clusterrole_clusterrbacassessments{name="clusterrole-779f88d9b5",severity="Medium"} 0
trivy_clusterrole_clusterrbacassessments{name="clusterrole-79d4fc89cd",severity="Critical"} 1
trivy_clusterrole_clusterrbacassessments{name="clusterrole-79d4fc89cd",severity="High"} 0
trivy_clusterrole_clusterrbacassessments{name="clusterrole-79d4fc89cd",severity="Low"} 0
trivy_clusterrole_clusterrbacassessments{name="clusterrole-79d4fc89cd",severity="Medium"} 0
trivy_clusterrole_clusterrbacassessments{name="clusterrole-79ff87886f",severity="Critical"} 0
trivy_clusterrole_clusterrbacassessments{name="clusterrole-79ff87886f",severity="High"} 0
trivy_clusterrole_clusterrbacassessments{name="clusterrole-79ff87886f",severity="Low"} 0
trivy_clusterrole_clusterrbacassessments{name="clusterrole-79ff87886f",severity="Medium"} 0
trivy_clusterrole_clusterrbacassessments{name="clusterrole-7b884bc5d8",severity="Critical"} 1
trivy_clusterrole_clusterrbacassessments{name="clusterrole-7b884bc5d8",severity="High"} 2
trivy_clusterrole_clusterrbacassessments{name="clusterrole-7b884bc5d8",severity="Low"} 0
trivy_clusterrole_clusterrbacassessments{name="clusterrole-7b884bc5d8",severity="Medium"} 1
trivy_clusterrole_clusterrbacassessments{name="clusterrole-7c4d8f665",severity="Critical"} 1
trivy_clusterrole_clusterrbacassessments{name="clusterrole-7c4d8f665",severity="High"} 1
trivy_clusterrole_clusterrbacassessments{name="clusterrole-7c4d8f665",severity="Low"} 0
trivy_clusterrole_clusterrbacassessments{name="clusterrole-7c4d8f665",severity="Medium"} 0
trivy_clusterrole_clusterrbacassessments{name="clusterrole-7c5d4b78b6",severity="Critical"} 0
trivy_clusterrole_clusterrbacassessments{name="clusterrole-7c5d4b78b6",severity="High"} 1
trivy_clusterrole_clusterrbacassessments{name="clusterrole-7c5d4b78b6",severity="Low"} 0
trivy_clusterrole_clusterrbacassessments{name="clusterrole-7c5d4b78b6",severity="Medium"} 0
trivy_clusterrole_clusterrbacassessments{name="clusterrole-7c7649d468",severity="Critical"} 0
trivy_clusterrole_clusterrbacassessments{name="clusterrole-7c7649d468",severity="High"} 0
trivy_clusterrole_clusterrbacassessments{name="clusterrole-7c7649d468",severity="Low"} 0
trivy_clusterrole_clusterrbacassessments{name="clusterrole-7c7649d468",severity="Medium"} 0
trivy_clusterrole_clusterrbacassessments{name="clusterrole-7dfccfdf",severity="Critical"} 0
trivy_clusterrole_clusterrbacassessments{name="clusterrole-7dfccfdf",severity="High"} 0
trivy_clusterrole_clusterrbacassessments{name="clusterrole-7dfccfdf",severity="Low"} 0
trivy_clusterrole_clusterrbacassessments{name="clusterrole-7dfccfdf",severity="Medium"} 0
trivy_clusterrole_clusterrbacassessments{name="clusterrole-7f76ddfb76",severity="Critical"} 0
trivy_clusterrole_clusterrbacassessments{name="clusterrole-7f76ddfb76",severity="High"} 0
trivy_clusterrole_clusterrbacassessments{name="clusterrole-7f76ddfb76",severity="Low"} 0
trivy_clusterrole_clusterrbacassessments{name="clusterrole-7f76ddfb76",severity="Medium"} 0
trivy_clusterrole_clusterrbacassessments{name="clusterrole-7f7cc8689f",severity="Critical"} 0
trivy_clusterrole_clusterrbacassessments{name="clusterrole-7f7cc8689f",severity="High"} 0
trivy_clusterrole_clusterrbacassessments{name="clusterrole-7f7cc8689f",severity="Low"} 0
trivy_clusterrole_clusterrbacassessments{name="clusterrole-7f7cc8689f",severity="Medium"} 0
trivy_clusterrole_clusterrbacassessments{name="clusterrole-7ff7dbc7fd",severity="Critical"} 0
trivy_clusterrole_clusterrbacassessments{name="clusterrole-7ff7dbc7fd",severity="High"} 0
trivy_clusterrole_clusterrbacassessments{name="clusterrole-7ff7dbc7fd",severity="Low"} 0
```

```
trivy_resource_configaudits{name="daemonset-prom-prometheus-node-exporter",namespace="monitoring",severity="Critical"} 0
trivy_resource_configaudits{name="daemonset-prom-prometheus-node-exporter",namespace="monitoring",severity="High"} 3
trivy_resource_configaudits{name="daemonset-prom-prometheus-node-exporter",namespace="monitoring",severity="Low"} 10
trivy_resource_configaudits{name="daemonset-prom-prometheus-node-exporter",namespace="monitoring",severity="Medium"} 2
trivy_resource_configaudits{name="daemonset-promtail",namespace="monitoring",severity="Critical"} 0
trivy_resource_configaudits{name="daemonset-promtail",namespace="monitoring",severity="High"} 0
trivy_resource_configaudits{name="daemonset-promtail",namespace="monitoring",severity="Low"} 8
trivy_resource_configaudits{name="daemonset-promtail",namespace="monitoring",severity="Medium"} 2
trivy_resource_configaudits{name="daemonset-tracee",namespace="tracee",severity="Critical"} 0
trivy_resource_configaudits{name="daemonset-tracee",namespace="tracee",severity="High"} 1
trivy_resource_configaudits{name="daemonset-tracee",namespace="tracee",severity="Low"} 6
trivy_resource_configaudits{name="daemonset-tracee",namespace="tracee",severity="Medium"} 3
trivy_resource_configaudits{name="replicaset-loki-loki-distributed-distributor-7cdbf467fc",namespace="monitoring",severity="Critical"} 0
trivy_resource_configaudits{name="replicaset-loki-loki-distributed-distributor-7cdbf467fc",namespace="monitoring",severity="High"} 0
trivy_resource_configaudits{name="replicaset-loki-loki-distributed-distributor-7cdbf467fc",namespace="monitoring",severity="Low"} 7
trivy_resource_configaudits{name="replicaset-loki-loki-distributed-distributor-7cdbf467fc",namespace="monitoring",severity="Medium"} 0
trivy_resource_configaudits{name="replicaset-loki-loki-distributed-gateway-6595fd6d55",namespace="monitoring",severity="Critical"} 0
trivy_resource_configaudits{name="replicaset-loki-loki-distributed-gateway-6595fd6d55",namespace="monitoring",severity="High"} 0
trivy_resource_configaudits{name="replicaset-loki-loki-distributed-gateway-6595fd6d55",namespace="monitoring",severity="Low"} 7
trivy_resource_configaudits{name="replicaset-loki-loki-distributed-gateway-6595fd6d55",namespace="monitoring",severity="Medium"} 0
trivy_resource_configaudits{name="replicaset-loki-loki-distributed-query-frontend-7dbd8b5d85",namespace="monitoring",severity="Critical"} 0
trivy_resource_configaudits{name="replicaset-loki-loki-distributed-query-frontend-7dbd8b5d85",namespace="monitoring",severity="High"} 0
trivy_resource_configaudits{name="replicaset-loki-loki-distributed-query-frontend-7dbd8b5d85",namespace="monitoring",severity="Low"} 7
trivy_resource_configaudits{name="replicaset-loki-loki-distributed-query-frontend-7dbd8b5d85",namespace="monitoring",severity="Medium"} 0
trivy_resource_configaudits{name="replicaset-prom-grafana-54894696b",namespace="monitoring",severity="Critical"} 0
trivy_resource_configaudits{name="replicaset-prom-grafana-54894696b",namespace="monitoring",severity="High"} 0
trivy_resource_configaudits{name="replicaset-prom-grafana-54894696b",namespace="monitoring",severity="Low"} 26
trivy_resource_configaudits{name="replicaset-prom-grafana-54894696b",namespace="monitoring",severity="Medium"} 6
trivy_resource_configaudits{name="replicaset-prom-kube-prometheus-stack-operator-64485f9567",namespace="monitoring",severity="Critical"} 0
trivy_resource_configaudits{name="replicaset-prom-kube-prometheus-stack-operator-64485f9567",namespace="monitoring",severity="High"} 0
trivy_resource_configaudits{name="replicaset-prom-kube-prometheus-stack-operator-64485f9567",namespace="monitoring",severity="Low"} 9
trivy_resource_configaudits{name="replicaset-prom-kube-prometheus-stack-operator-64485f9567",namespace="monitoring",severity="Medium"} 0
trivy_resource_configaudits{name="replicaset-prom-kube-state-metrics-86965c46b8",namespace="monitoring",severity="Critical"} 0
trivy_resource_configaudits{name="replicaset-prom-kube-state-metrics-86965c46b8",namespace="monitoring",severity="High"} 0
trivy_resource_configaudits{name="replicaset-prom-kube-state-metrics-86965c46b8",namespace="monitoring",severity="Low"} 10
trivy_resource_configaudits{name="replicaset-prom-kube-state-metrics-86965c46b8",namespace="monitoring",severity="Medium"} 2
trivy_resource_configaudits{name="statefulset-cfdb49d85",namespace="monitoring",severity="Critical"} 0
trivy_resource_configaudits{name="statefulset-cfdb49d85",namespace="monitoring",severity="High"} 0
trivy_resource_configaudits{name="statefulset-cfdb49d85",namespace="monitoring",severity="Low"} 8
trivy_resource_configaudits{name="statefulset-cfdb49d85",namespace="monitoring",severity="Medium"} 0
trivy_resource_configaudits{name="statefulset-loki-loki-distributed-ingester",namespace="monitoring",severity="Critical"} 0
trivy_resource_configaudits{name="statefulset-loki-loki-distributed-ingester",namespace="monitoring",severity="High"} 0
trivy_resource_configaudits{name="statefulset-loki-loki-distributed-ingester",namespace="monitoring",severity="Low"} 7
trivy_resource_configaudits{name="statefulset-loki-loki-distributed-ingester",namespace="monitoring",severity="Medium"} 0
trivy_resource_configaudits{name="statefulset-loki-loki-distributed-querier",namespace="monitoring",severity="Critical"} 0
trivy_resource_configaudits{name="statefulset-loki-loki-distributed-querier",namespace="monitoring",severity="High"} 0
trivy_resource_configaudits{name="statefulset-loki-loki-distributed-querier",namespace="monitoring",severity="Low"} 7
trivy_resource_configaudits{name="statefulset-loki-loki-distributed-querier",namespace="monitoring",severity="Medium"} 0
trivy_resource_configaudits{name="statefulset-prometheus-prom-kube-prometheus-stack-prometheus",namespace="monitoring",severity="Critical"} 0
trivy_resource_configaudits{name="statefulset-prometheus-prom-kube-prometheus-stack-prometheus",namespace="monitoring",severity="High"} 0
trivy_resource_configaudits{name="statefulset-prometheus-prom-kube-prometheus-stack-prometheus",namespace="monitoring",severity="Low"} 11
trivy_resource_configaudits{name="statefulset-prometheus-prom-kube-prometheus-stack-prometheus",namespace="monitoring",severity="Medium"} 0
```

Step 4 Setting up a dashboard

The dashboard can be found in the following repo: https://grafana.com/grafana/dashboards/16652-trivy-operator-reports/

Step 5 Avoiding Vulnerability Hell

Tweet https://twitter.com/AlexJonesax/status/1569998923955142657

Some possible strategies

1. Ignore all but Critical Vulnerabilities
2. Don't scan everything at once
3. Filter by Vulnerabilities with known-fixture
4. Filter Vulnerabilities by team & by application
5. Make the Vulnerabilities context-specific

Step 6 What are metrics without alerts

aqua

State	Name	Health	Summary
Normal	Critical Vulnerability	ok	

Silence | Show state history | View | Edit | Delete

Evaluate: Every 1m

For: 5m

Data source: Prometheus

Matching instances

Search by label: Search

State: Normal 1 | Alerting | Pending | NoData | Error

State	Labels	Created
Normal	alertname=Critical Vulnerability, grafana_folder=test	-

@urlichsanais

aqua

It's easy to ignore vulnerabilities – give them a "voice"

Step 7 Correlating Metrics

aqua

General / Trivy Operator Reports

Last 1 hour | 30s

datasource: Prometheus | Cluster: All | namespace: All

Summary of vulnerabilities

LOW	MEDIUM	HIGH	CRITICAL	UNKNOWN	TOTAL
8	76	124	24	12	244

All vulnerabilities by namespaces

All vulnerabilities by severity

Summary Resource Config Audit

LOW	MEDIUM	HIGH	CRITICAL	TOTAL
131	17	4	0	152

All config audits by namespaces

All config audits by severity

@urlichsanais

Replicas available by deployment
2022-10-11 16:49:00
cilium-operator 1
coredns 2
loki-loki-distributed-distributor 1
loki-loki-distributed-gateway 1
loki-loki-distributed-query-frontend 1
prom-grafana 1
prom-kube-prometheus-stack-operator 1
prom-kube-state-metrics 1
react-application 2
trivy-operator 1

General / Kubernetes / Views / Namespaces
2022-10-11 16:43:31 to 2022-10-11 16:49:46
datasource Prometheus
namespace All
resolution 30s
Overview
Namespace(s) usage on total cluster CPU in %
27.38%
Namespace(s) usage on total cluster RAM in %
42.39%
Kubernetes Resource Count
Min Max Mean
Secrets 76 77 76.4
Running Pods 48 50 48.8
Configmaps 48 49 48.4
Services 24 25 24.4
Deployments 9 10 9.38
Daemonsets 9 9 9
Statefulsets 4 4 4
Namespace(s) CPU Usage in cores
Real Requests Limits Cluster Total
3.03 3.68 2.93 6
Namespace(s) RAM Usage in bytes
Real Requests Limits Cluster Total
4.95 GiB 2.98 GiB 2.91 GiB 11.5 GiB
Resources
CPU usage by Pod
CPU Cores
alertmanager-prom-kube-prometheus-stack-alertmanager-0
cilium-62kht
cilium-c2fsz
cilium-ds7k6
cilium-operator-6478464bd7-fxvdv
coredns-9c8d9dc8c-8pslt
coredns-9c8d9dc8c-ld9t6
cpc-bridge-proxy-74cqw
cpc-bridge-proxy-nvxkv
cpc-bridge-proxy-zcbnf
Memory usage by Pod

Step 8 Some additional tips

Just a few more things to think about...

- Assign Ownership
- Don't introduce "too many" new tools at once
- Utilise existing workflows, platforms and processes

Step 9 Optimise based on what works for your team

aqua

The initial setup might be the same but everything else will be different

Step 10 Don't stop at security scanning

https://github.com/aquasecurity/tracee

aqua tracee

@urlichsanais

Additional Resources

- Our Application Security Journey (Part 1) by Wise Engineering
- The Aqua Open Source YouTube Channel
- The Trivy GitHub Repository and the Trivy Operator Repository
- The demo project on GitHub

& You can find us on Slack: slack.aquasec.com

Questions

@urlichsanais

Thanks

@urlichsanais