KubeCon | CloudNativeCon

Europe 2023

Nurturing Security Permaculture

Kubernetes SIG Security Update

Ala Dewberry, Savitha Raghunathan, Tabitha Sable, Mahé Tardy

KubeCon | CloudNativeCon
Europe 2023

Documentation

Savitha Raghunathan

Documentation

- Sub Project Goals:

  - Collaborate and create/improve existing security content for Kubernetes documentation.
  - Keep the documentation and security examples up to date.
  - Create security awareness through documentation.

- Current Projects:

  - Hardening guide
  - Blog post on Confidential Computing
  - Ongoing updates to the Kubernetes website.

Docs: What's Next?

- Future Projects:

  - Update Kubernetes security checklist application deployment.
  - Kubernetes RBAC guide and tutorial.

- sig-security-docs subproject is looking for volunteers!

- If you have an idea to improve the security content of Kubernetes website, please feel free to start a thread in the slack channel and/or create an issue in the k/website repo.

Third-Party Audit

Audit

Subproject Goals:

- Coordinate regular, comprehensive, third-party security audits

Audit Goals:

- Identify vulnerabilities or weaknesses in Kubernetes
- Make Kubernetes more secure

Audit Status

- Report is now public!
    - Find it in kubernetes/sig-security repo on GitHub
- Findings addressed before publication as appropriate
    - 6 medium severity issues
    - 9 low severity issues
    - 4 informational findings
- Thank you to everyone involved
    - NCC Group staff
    - Subgroup members
    - SRC and SIG members

KubeCon | CloudNativeCon

Europe 2023

Tooling

Mahé Tardy

What is tooling subproject?

Goals:

- Build and improve security by working across SIGs and other sub-projects.
- Create space for **new contributors** to share and learn.

Meeting organization: Two times a month on Wednesdays (8:00am PDT, 17:00 CEST)

- 1st meeting: **working session** - we go through issues, PRs together and find opportunities for new members to contribute.
- 2nd meeting: **learning session** - we invite members and guests from other SIGs to present deep dives, code walkthroughs and demos on topics that align with our SIG charter. (No vendor pitches / demos). You can be a speaker too! Add yourself to the list and present during learning sessions.

Date	Topic	Speaker(s)	Link
03-29-2023	Copacetic	Xander Grzywinski	https://www.youtube.com/watch?v=6Be41Nf52ts
03-01-2023	Security-Guard	David Hadas	https://youtu.be/FNIdRBGwzOo
08-16-2022	KubeAudit	Genevieve Luyt & Dani Santos	https://youtu.be/m18AIFmfM00
07-05-2022	Eraser	Xander Grzywinski	https://youtu.be/c1yhWxxEkJI
04-19-2022	Stratus Red Team	Christophe Tafani-Dereeper	https://youtu.be/qb59dvq4KYE
03-15-2022	SIG Security	Pushkar Joglekar	https://youtu.be/jqfDgaGqJX0

What does tooling subproject do?

CVE Feed

- JSON CVE feed now complies with JSON Feed specification v1.1
- CVE feed now additionally supports RSS format
- Metadata Updates:
  - Timestamp added to indicate freshness
  - URL of feed refresh cron job

CVE Scanner *(looking for new maintainers!)*

- Build Time (Go modules) and Release Image Scanning for k/k repo:
  - Running since last 18 months; every 6 hours
  - Please reach out to #sig-security-tooling, if you’d like to know more

Ref: https://kubernetes.io/docs/reference/issues-security/official-cve-feed/ https://github.com/kubernetes/sig-security/tree/main/sig-security-tooling/vulnerability-mgmt

Self Assessments

Ala Dewberry

Self Assessments

For a Single Self Assessment:

To answer two questions -

- What is the security posture of the workflow modelled?
- How can we improve it?

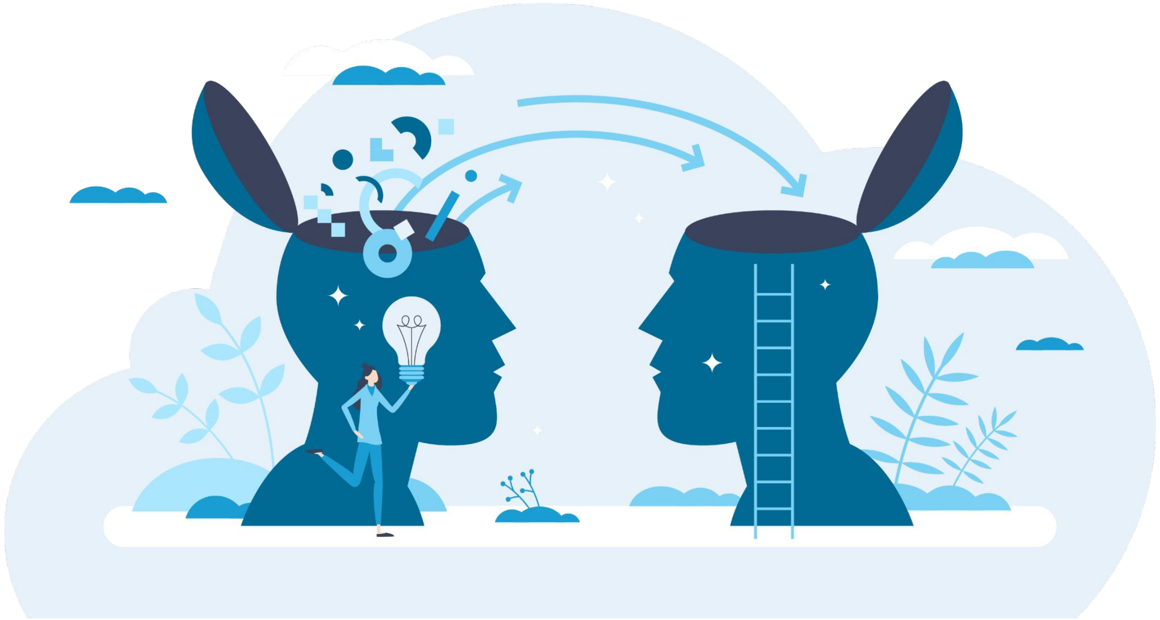
…And capture actions to take to improve the security posture

For the Project:

- Fill the Repo! Self Assessments for all Projects and Subprojects

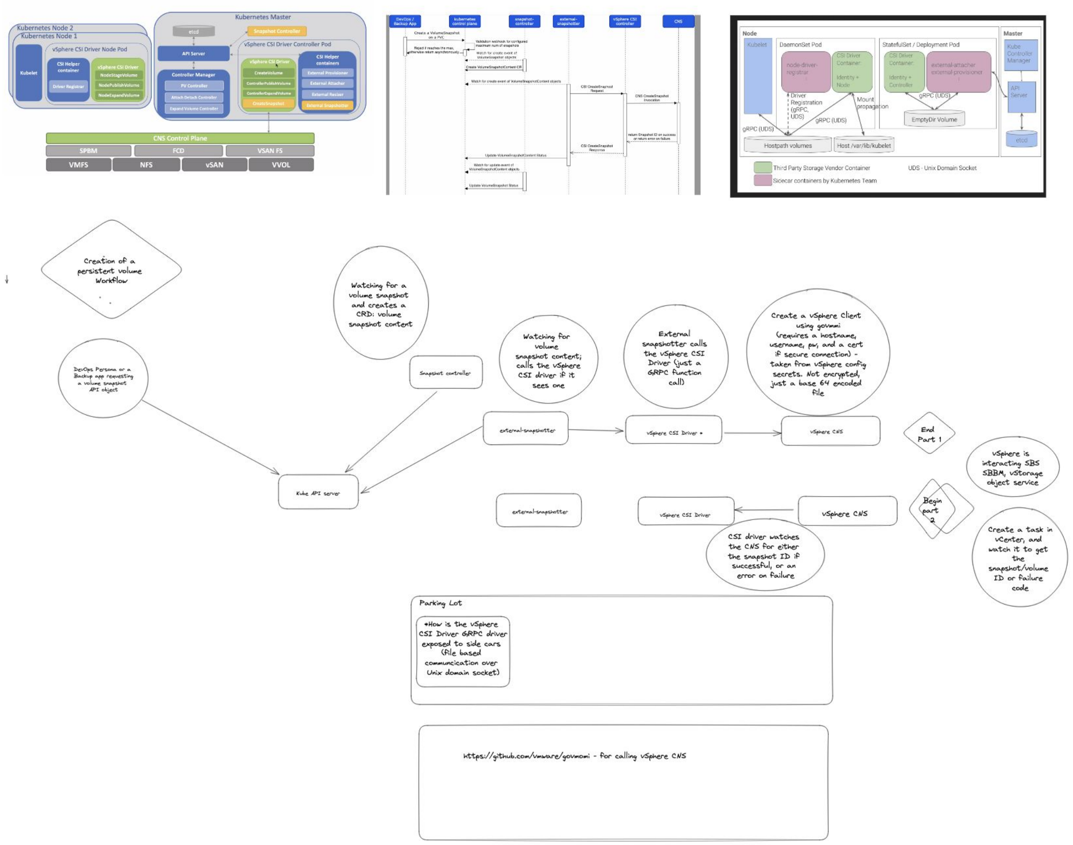
Why are Self Assessments Important?

- Positively augment the security posture of Kubernetes
- Knowledge Sharing
- Building Security Muscle in Kubernetes Community



What Have We Been Up To?

- vSPhere CSI Driver Self Assessment!
- First Session Complete - Data Flow Diagram Complete for Creations of a persistent volume
- Next Steps:
  - Continue with next workflows
  - Note encryption on data flows, label ports
  - Apply STRIDE model
  - Perform write up, submit for feedback, publish!
  - (Potentially: Queue up Fuzzing exercise)
  - …Find our next project!


Kubernetes Node 2
Kubernetes Node 1
Kubelet
vSphere CSI Driver Node Pod
CSI Helper container
Driver Registrar
vSphere CSI Driver
NodeStageVolume
NodePublishVolume
NodeExpandVolume
Kubernetes Master
etcd
Snapshot Controller
API Server
Controller Manager
PV Controller
Attach Detach Controller
Expand Volume Controller
vSphere CSI Driver Controller Pod
vSphere CSI Driver
CreateVolume
ControllerPublishVolume
ControllerExpandVolume
CreateSnapshot
CSI Helper containers
External Provisioner
External Attacher
External Resizer
External Snapshotter
CNS Control Plane
SPBM
FCD
VSAN FS
VMFS
NFS
vSAN
VVOL
DevOps / Backup App
kubernetes control plane
snapshot-controller
external-snapshotter
vSphere CSI controller
CNS
Create a VolumeSnapshot on a PVC
Validation webhook for configured maximum num of snapshots
Reject if reaches the max, otherwise return asynchronously
Watch for create event of VolumeSnapshot objects
Create VolumeSnapshotContent CR
Watch for create event of VolumeSnapshotContent objects
CSI CreateSnapshot Request
CNS CreateSnapshot Invocation
return Snapshot ID on success or return error on failure
CSI CreateSnapshot Response
Update VolumeSnapshotContent Status
Watch for update event of VolumeSnapshotContent objects
Update VolumeSnapshot Status
Node
Kubelet
DaemonSet Pod
node-driver-registrar
CSI Driver Container
Identity + Node
Driver Registration (gRPC, UDS)
gRPC (UDS)
gRPC (UDS)
Mount propagation
StatefulSet / Deployment Pod
CSI Driver Container
Identity + Controller
external-attacher external-provisioner
gRPC (UDS)
EmptyDir Volume
Hostpath volumes
Host /var/lib/kubelet
Master
Kube Controller Manager
API Server
etcd
Third Party Storage Vendor Container
Sidecar containers by Kubernetes Team
UDS - Unix Domain Socket
Creation of a persistent volume Workflow
DevOps Persona or a Backup app requesting a volume snapshot API object
Watching for a volume snapshot and creates a CRD: volume snapshot content
Snapshot controller
Watching for volume snapshot content; calls the vSphere CSI driver if it sees one
External snapshotter calls the vSphere CSI Driver (just a GRPC function call)
Create a vSphere Client using govmmi (requires a hostname, username, pw, and a cert if secure connection) - taken from vSphere config secrets. Not encrypted, just a base 64 encoded file
Kube API server
external-snapshotter
vSphere CSI Driver *
vSphere CNS
End Part 1
vSphere is interacting SBS SBBM, vStorage object service
external-snapshotter
vSphere CSI Driver
vSphere CNS
Begin part 2
CSI driver watches the CNS for either the snapshot ID if successful, or an error on failure
Create a task in vCenter, and watch it to get the snapshot/volume ID or failure code
Parking Lot
*How is the vSphere CSI Driver GRPC driver exposed to side cars (file based communcication over Unix domain socket)
https://github.com/vmware/govmomi - for calling vSphere CNS

Where Are We Going?

- Guiding Metric: Fill the repo! Are you next? Submit a Request!

- Feel free to listen in on the vSphere CSI Driver sessions - Sessions Scheduled in Slack via Doodle

- If you have experience, be a guide! DM Ala on Kubernetes Slack (Ala Dewberry)

Security Permaculture?!

Why Permaculture?

- Intentional
- Holistic
- Systematic
- Self-regulating
- Self-sustaining

What if “security culture” were more like permaculture?

How do we do it?

- Inclusion
  - Form community together
  - Create opportunities to lead and support
- Collective action
  - Decisions via loose consensus
  - What gets done depends on who participates
  - What we do, we do together
- Support, not authority
  - Make code changes together with owning SIGs
  - Suggest improvements, assist implementation

...and you can, too!

- #sig-security on Kubernetes slack
- Meetings bi-weekly, Thursdays 6:00PM CEST (9:00AM US/Pacific)
  - Join email group to receive meeting invitations

Thank You!

KubeCon | CloudNativeCon

Europe 2023

Please scan the QR Code above
to leave feedback on this session