

DIGITAL FORENSICS WITH CONTAINER CHECKPOINTING

Daniel Simionato and Javier Martínez

#OSSummit



@



THE LINUX FOUNDATION

EUROPE



ABOUT US

Daniel Simionato and Javier Martínez



WHAT IS DIGITAL FORENSICS?

WHAT IS DIGITAL FORENSICS?

It's the process of...

WHAT IS DIGITAL FORENSICS?

It's the process of...

- retrieving

WHAT IS DIGITAL FORENSICS?

It's the process of...

- retrieving
- analyzing

WHAT IS DIGITAL FORENSICS?

It's the process of...

- retrieving
- analyzing
- preserving

WHAT IS DIGITAL FORENSICS?

It's the process of...

- retrieving
- analyzing
- preserving

electronic data as evidence of a criminal activity

DFIR

Digital Forensics

+

Incident Response

CRIMINAL ACTIVITY



CRIMINAL ACTIVITY

- Cryptojacking



CRIMINAL ACTIVITY

- Cryptojacking
- Malware



CRIMINAL ACTIVITY

- Cryptojacking
- Malware
- Ransomware
- ...





CONTAINER CHECKPOINTING



CONTAINER CHECKPOINTING

- Save the current container state



CONTAINER CHECKPOINTING

- Save the current container state
- Snapshot



CONTAINER CHECKPOINTING

- Save the current container state
- Snapshot
- Backup



HOW CHECKPOINTING IS USEFUL FOR DFIR?

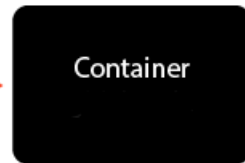
Investigate a container

HOW CHECKPOINTING IS USEFUL FOR DFIR?

Investigate a container
and retrieve **criminal evidence**

HOW CHECKPOINTING IS USEFUL FOR DFIR?

Investigate a container
and retrieve **criminal evidence**
while the attacker is **unaware**



CHECKPOINT

Checkpoint
image

- history commands
- files modified
- attacker path
- network connection
- memory
- ...

IT ALL STARTED WITH CRIU



IT ALL STARTED WITH CRIU

- Initial POC on 2011



IT ALL STARTED WITH CRIU

- Initial POC on 2011
- Started from Virtuozzo



IT ALL STARTED WITH CRIU

- Initial POC on 2011
- Started from Virtuozzo
- 1.0 in Nov. 2013 (Linux 3.11)



IT ALL STARTED WITH CRIU

- Initial POC on 2011
- Started from Virtuozzo
- 1.0 in Nov. 2013 (Linux 3.11)
- Checkpoint/Restore In Userspace



IT ALL STARTED WITH CRIU

- Initial POC on 2011
- Started from Virtuozzo
- 1.0 in Nov. 2013 (Linux 3.11)
- Checkpoint/Restore In Userspace
- Multiple use cases




CONTAINER CHECKPOINT DEMO






CHECKPOINTING IN KUBERNETES

Graduated to alpha in Kubernetes v1.25 (#2008)

Forensic Container Checkpointing #2008



 **Open** adrianreber opened this issue on Sep 23, 2020 · 51 comments

**adrianreber** commented on Sep 23, 2020 · edited 

Contributor · 

Enhancement Description

- One-line enhancement description (can be used as a release note): Forensic Container Checkpointing
- Kubernetes Enhancement Proposal: [🔗 Add Forensic Container Checkpointing KEP #1990](#)
- Discussion Link:
 - SIG Node weekly meeting: <https://docs.google.com/document/d/1Ne57gvidMEWXR70OxxnRkYquAoMpt56o75oZtg-OeBg/edit>
 - SIG Node planning doc for v1.23: <https://docs.google.com/document/d/1U10J0WwgWXkdYrqWGGvO8iH2HKeerQAlygnqgDgWv4E/edit>
- Primary contact (assignee): [@adrianreber](#)
- Responsible SIGs: Sig Node
- Enhancement target (which target equals to which milestone): No target so far
 - Alpha release target (x.y): 1.24
 - Beta release target (x.y): 1.25
 - Stable release target (x.y): 1.27

  12

CHECKPOINTING IN KUBERNETES

Currently only checkpointing

Restore still not available

CHECKPOINT PROCEDURE

We call Kubernetes API:

```
POST /checkpoint/{namespace}/{pod}/{container}
```

Kubelet will request a checkpoint

A .tar file is created under:

```
/var/lib/kubelet/checkpoints
```


CHECKPOINTING IN KUBERNETES

REQUIREMENTS: ENABLE CRI-O AND CRIU

CHECKPOINTING IN KUBERNETES

REQUIREMENTS: ENABLE CRI-O AND CRIO

- Container runtime: CRI-O

CHECKPOINTING IN KUBERNETES

REQUIREMENTS: ENABLE CRI-O AND CRIU

- Container runtime: CRI-O
- Enable feature gate: ContainerCheckpoint

```
--feature-gates=ContainerCheckpoint=True
```

CHECKPOINTING IN KUBERNETES

REQUIREMENTS: ENABLE CRI-O AND CRIU

- Container runtime: CRI-O
- Enable feature gate: ContainerCheckpoint

```
--feature-gates=ContainerCheckpoint=True
```

- Enable CRIU support in the config

```
enable_criu_support = true
```

KUBERNETES CHECKPOINT OUTPUT

KUBERNETES CHECKPOINT OUTPUT

A tar file, containing

KUBERNETES CHECKPOINT OUTPUT

A tar file, containing

- Archive of all changed files (rootfs-diffs.tar)

KUBERNETES CHECKPOINT OUTPUT

A tar file, containing

- Archive of all changed files (rootfs-diffs.tar)
- Images (of processes, memory, file descriptors...)

KUBERNETES CHECKPOINT OUTPUT

A tar file, containing

- Archive of all changed files (rootfs-diffs.tar)
- Images (of processes, memory, file descriptors...)
- Metadata

KUBERNETES CHECKPOINT OUTPUT

A tar file, containing

- Archive of all changed files (rootfs-diffs.tar)
- Images (of processes, memory, file descriptors...)
- Metadata
- Bind mounts info

KUBERNETES CHECKPOINT OUTPUT

A tar file, containing

- Archive of all changed files (rootfs-diffs.tar)
- Images (of processes, memory, file descriptors...)
- Metadata
- Bind mounts info
- Stats&logs

KUBERNETES CHECKPOINT DEMO



CHECKPOINTCTL DEMO



CHECKPOINT ANALYSIS & CRIT DEMO



CHECKPOINTING IN KUBERNETES

CHECKPOINTING IN KUBERNETES

- The copy is created without the container knowing

CHECKPOINTING IN KUBERNETES

- The copy is created without the container knowing
- No processes are stopped

RESTORING

RESTORING

- Load container state in a sandbox

RESTORING

- Load container state in a sandbox
- Outside of k8s: Podman

RESTORING

- Load container state in a sandbox
- Outside of k8s: Podman
- Inside of k8s: build an image from the checkpoint

CRIU LIMITATIONS

Not everything can be checkpointed:

CRIU LIMITATIONS

Not everything can be checkpointed:

- Devices

CRIU LIMITATIONS

Not everything can be checkpointed:

- Devices
- Open files from unmounted fs

CRIU LIMITATIONS

Not everything can be checkpointed:

- Devices
- Open files from unmounted fs
- Traced processes

KUBERNETES CHECKPOINTING LIMITATIONS

KUBERNETES CHECKPOINTING LIMITATIONS

- CRI-O has to be enabled

KUBERNETES CHECKPOINTING LIMITATIONS

- CRI-O has to be enabled
- Needs criu v3.16+

KUBERNETES CHECKPOINTING LIMITATIONS

- CRI-O has to be enabled
- Needs criu v3.16+
- Containerd

OTHER USAGES

- Backups
- Recovery from failure
- Container migration

SUMMARY

- Checkpoint can be crucial in DFIR
- Snapshot of a container state
- Checkpointing available in K8s
- Beware of requirements

THANK YOU!

QUESTIONS

?

