

Policy Was **Never Reapplied** on Restore

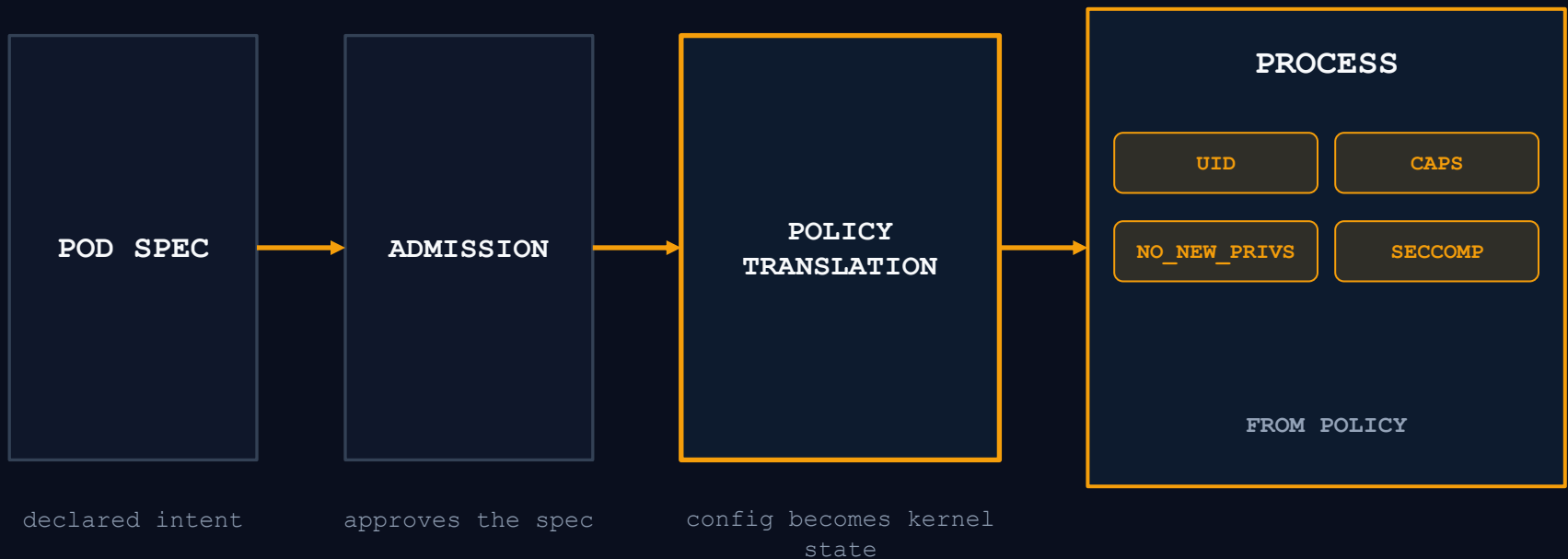
How a checkpoint restore can return a process admission never approved



Creation applies **policy**

Pod spec, admission, runtime translation. Policy becomes uid, capabilities, no_new_privs, seccomp.

CREATE PATH

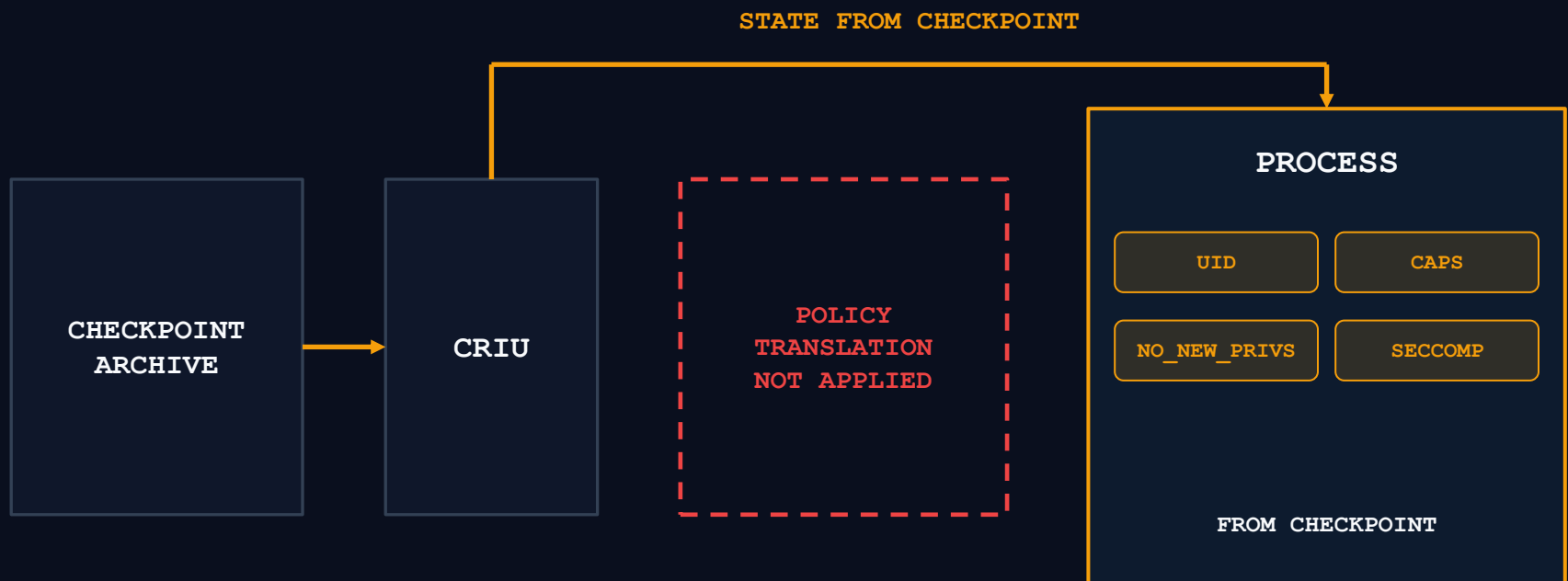


EVERY ATTRIBUTE ON THE PROCESS TRACES BACK TO THE SPEC

Restore **reconstitutes** instead

On the affected containerd path, saved credentials, capabilities, no_new_privs and seccomp state come from the checkpoint.

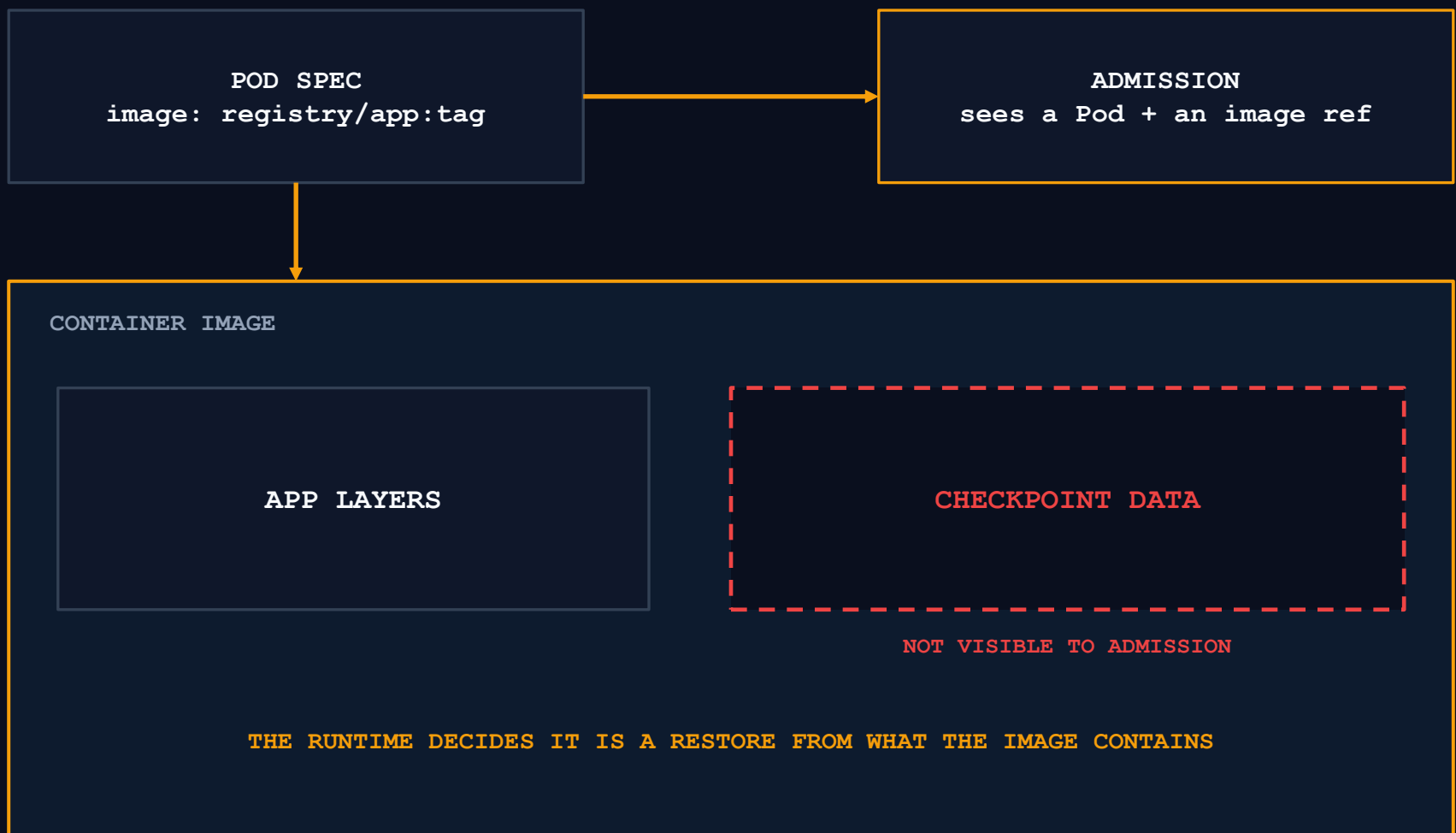
RESTORE PATH



THE TRANSLATION STEP IS NOT ON THIS ROUTE

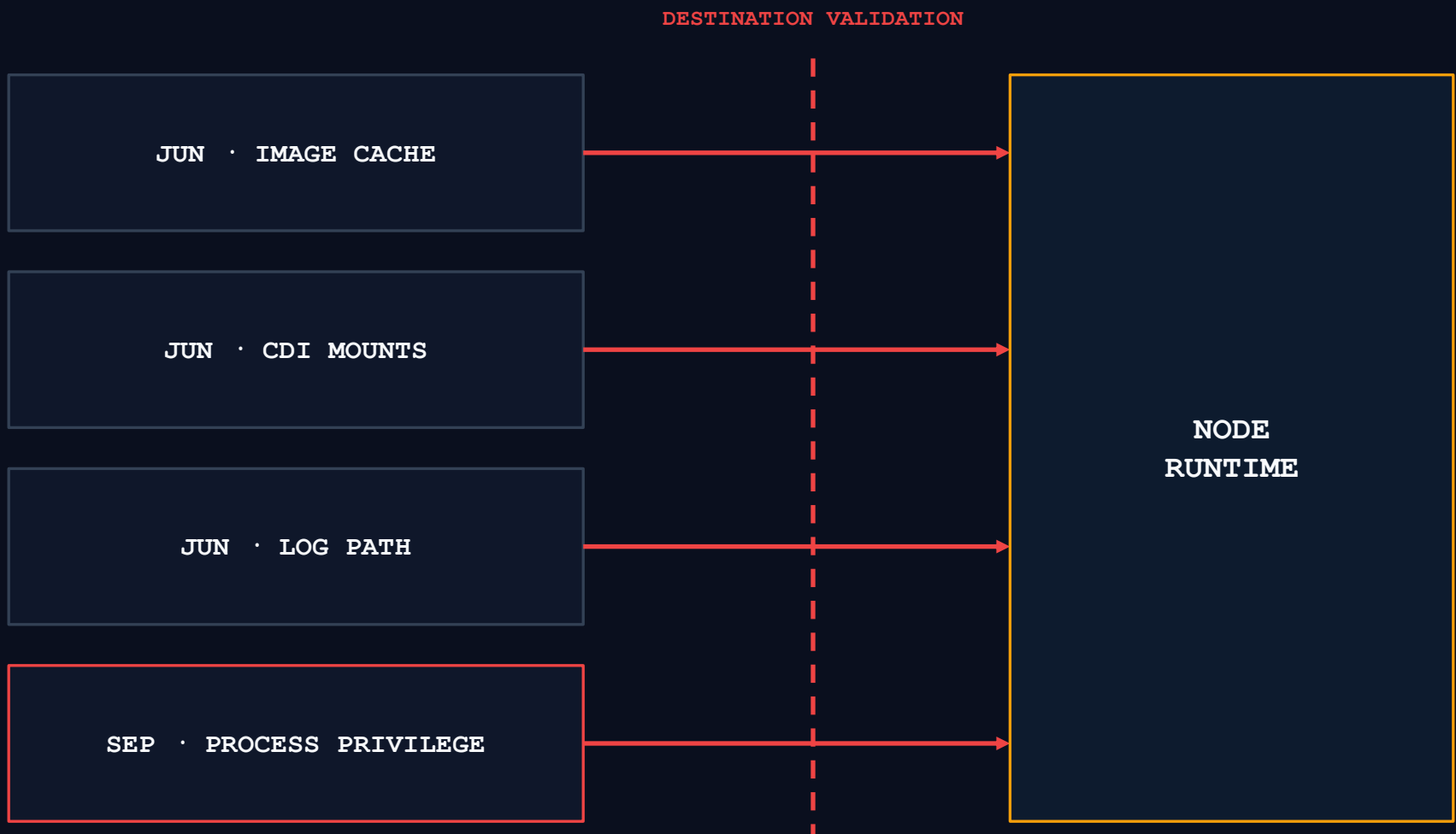
Admission sees an **ordinary** create

A Pod with an image reference. The runtime decides it is a restore from what the image contains.



Four advisories, **one boundary**

Image references, CDI mounts, log paths, process privilege. Four different bugs. Checkpoint-supplied input crossed destination validation.



Precedence was **never** decided

Nothing weighed saved state against requested policy. A chosen rule can be audited. A missing one has to be built.



ON THE AFFECTED PATH: SAVED STATE TAKES EFFECT

Status reports the **request**

containerd's status reflected the requested config, not the restored process.
Read NoNewPrivs, Seccomp and CapEff from /proc.

POD SPEC · REQUESTED

seccomp: RuntimeDefault

allowPrivilegeEscalation: false

capabilities: drop ALL

≠

/proc/<pid>/status · EFFECTIVE

Seccomp: 0

NoNewPrivs: 0

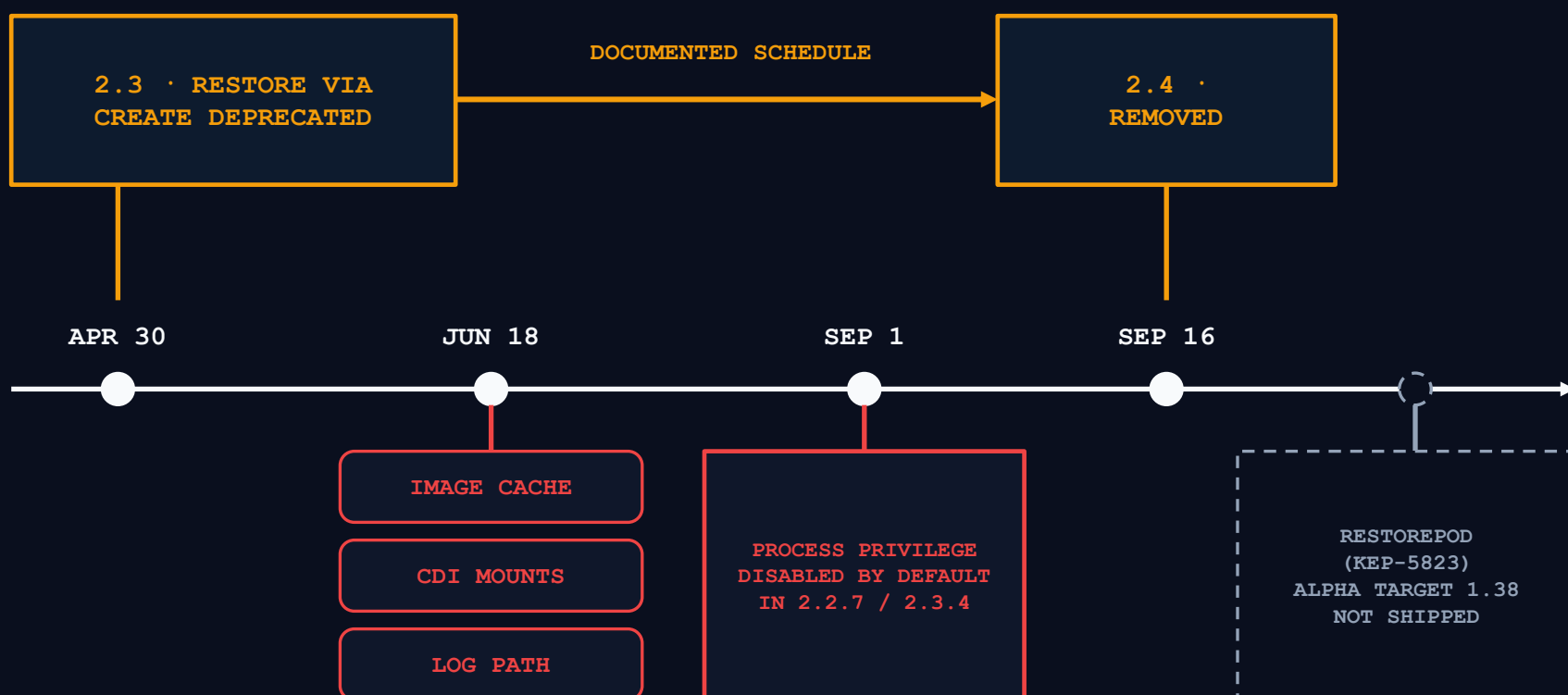
CapEff: full set

STATUS: REQUESTED CONFIG

ILLUSTRATIVE VALUES

The removal was **already scheduled**

Restore through create: deprecated in 2.3, removed in 2.4. The explicit replacement, KEP-5823, has not shipped.



What restore has to **prove**

Admission cannot supply this proof. Three things have to be shown before a restored process is trusted.



Requested deliberately

by someone allowed to request it



From a trusted source

artifact provenance and registry control



Effective state matches policy

read from the process, not the spec

[READ THE PROCESS](#)

Admission decides what a workload may be.

Restore decides what it becomes when nobody asks.

rack2cloud.com | Follow The Architect for more