Cursor Agent Box — Technical Summary

Collected: 2026-08-12

Environment: shared agent computer used by Grok Bot / Cursor agents

Hostname: `cursor`

Classification: Confirmed vs Inferred labeled throughout. Secrets redacted.

---

1. Executive stack

```
[AWS us-west-2 egress / multi-EIP SNAT pool]     ← CONFIRMED
        ↑
[Firecracker microVM on KVM]                     ← CONFIRMED
   root=/dev/vda · console=ttyS0 · nomodule · SWAP_SIZE_MB=0
        ↑
[Docker Engine + overlay2 rootfs]                ← CONFIRMED
   /.dockerenv · ~65 overlay lowers · docker0
        ↑
[Container PID1: tini → pod-daemon]              ← CONFIRMED
        ↑
[sand-exit-watch + exec-daemon + sand-host
 + multi Xvfb agent desktops]
```

This is neither a bare EC2 guest nor a plain desktop container alone. Live inspection shows a **Firecracker microVM** hosting a **Docker-style containerized agent runtime** (on-box docs refer to an "anyrun" path as alternate; this instance has `/.dockerenv`).

---

2. Virtualization — Firecracker evidence

Confirmed

Signal	Observation
Hypervisor	KVM (`lscpu`; dmesg: "Hypervisor detected: KVM")
ACPI OEM / table IDs	`FIRECK`, `FCMVXSDT`, `FCVMFADT`, `FCVMDSDT`, … OEM rev `FCAT 20240119`
DMI / SMBIOS	Empty / invalid (classic Firecracker)
Root disk	`/dev/vda` 128 GiB virtio-blk
Virtio devices	balloon, block, net (`enp0s3`), **vsock**, RNG
Console	Serial `/dev/ttyS0`; cmdline `earlyprintk=ttyS0`
Clock	`clocksource=kvm-clock`, `tsc=unstable`
Modules	`nomodule` + `modules_disabled=1`
Swap	Explicitly disabled (`SWAP_SIZE_MB=0`; `SwapTotal=0`)
Nitro / ENA	No Amazon Nitro / `ena` strings in sampled dmesg

Verdict (CONFIRMED): Firecracker microVM — not Nitro guest branding, not plain QEMU desktop branding.

Kernel cmdline (selected knobs)

Static guest IP `172.30.0.2/24` via `172.30.0.1`, cgroup v2, `reboot=k panic=1`, headless `i8042.*` flags, `random.trust_cpu=on`.

Kernel: `Linux cursor 6.12.94+` (custom build, Debian 12 gcc toolchain).

Inferred

- Guest CPUID model **207 (0xCF)** → Intel **Emerald Rapids–class** Xeon; SKU string sanitized to generic "Intel(R) Xeon(R) Processor".
- Exact AWS substrate under Firecracker (metal Nitro host vs other control plane) is **not** visible from inside the guest.

---

3. Container / pod layer

Confirmed markers

Signal	Result
`/.dockerenv`	Present (0-byte)
Root filesystem	`overlay` with **~65** Docker `overlay2` lowerdirs
`docker0`	`172.17.0.1/16` (DOWN / NO-CARRIER — no child containers)
Listen `:2375`	Present on `0.0.0.0` (Docker API–style port)
`docker` CLI	**Not** in PATH for the `box` user
PID 1	`/tini -- /pod-daemon … --ssh-auth-vsock-port 52`
cgroup	v2 path `0::/agent`; memory.max = 16 GiB; cpu.max = 8.0 CPUs

Control-plane tree (abbreviated)

```
tini
 └─ pod-daemon (vsock SSH auth :52)
     └─ sand-exit-watch
         ├─ exec-daemon :1337 / :1338   (computer-use, MCP meta)
         ├─ sand-supervisor → sand-host host-main.cjs :1340
         ├─ sand-window-router / session-sync / cookie-persist
         ├─ websockify :6081 (tokenized multi-desktop)
         └─ start-desktop.sh × N
             ├─ Xvfb :N
             ├─ x11vnc (localhost)
             ├─ xfwm4 + picom + plank
             └─ (on demand) Chrome → chrome-profile-N
```

`sand-host` version observed: `e6e3bb2`. Cluster env: `SAND_BOX_CLUSTER=us9`, store backend `v2`.

Inferred / open

Whether `:2375` is a live Docker Engine or a shim is unknown (port open, CLI missing, `docker0` empty). Host `/var/lib/docker/...` paths appear in mount options but are not listable as the `box` user.

---

4. Compute & storage

Confirmed

Resource	Value
vCPUs	8 (1 socket, 8 cores, 1 thread/core — no HT exposed)
Frequency	2400.000 MHz (fixed / `tsc_known_freq`)
RAM	~16 GiB MemTotal; cgroup-capped at exactly 16 GiB
NUMA	Single faked `node0`
Disk	128 GiB virtio; overlay `/` ~126 G usable, ~7–8% used at collection
`/dev`, `/dev/shm`	64 MiB tmpfs each
CPU features	Full AVX-512 set + AMX (`amx_bf16` / `amx_tile` / `amx_int8`); `vmx` advertised

Inferred: Large guest L3 (320 MiB) is consistent with a big host Xeon sliced thinly.

Persistence (product behavior)

Class	Label
`/workspace` and `/home/box` persist across agent turns	CONFIRMED (docs + observation)
"Update Grok Bot’s Computer" keeps files and logins	CONFIRMED documented
"Reset" restores snapshot (can lose unsynced work)	CONFIRMED documented
Shared FS across agents on this machine	CONFIRMED product model

Scratch `/workspace` was ~65 M; `/home/box` ~1.8 G (large Chrome profiles dominate).

---

5. Multi-desktop model

Confirmed: One shared VM/container; multiple logical agent windows (`SAND_BOX_MAX_WINDOWS=100`). At collection, at least three displays were live:

Display	Stack
`:1`	Xvfb 1280×800×24 · x11vnc `:5900` · websockify `:6080`
`:2`	Same pattern (`DISPLAY=:2` for this session) · VNC `:5902`
`:3`	Present in ports/logs · VNC `:5903` · Chrome CDP etc.

Desktops are isolated by **X display** and **Chrome profile**. Filesystem (`/home/box`, `/workspace`) is **shared** across agents. Session bus: `dbus-daemon`. No PulseAudio/PipeWire server process (client libs only). Wayland unset — X11 only.

---

6. Network, egress, and IMDS

Addressing — Confirmed

Item	Value
Primary IF	`enp0s3` (virtio-net), MTU 1500
IPv4	`172.30.0.2/24`
Gateway	`172.30.0.1`
DNS	`10.0.0.2` (Docker-engine-style `resolv.conf`)
Proxy env	None (`HTTP_PROXY` unset)

Egress — Confirmed

Public checkers in one session returned **distinct** AWS addresses, all **AS16509 / us-west-2 (Oregon / Boardman)**. Behavior matches a connection-hashed **SNAT / NAT gateway pool** (not a single sticky EIP). Optional on-box binary `sand-egress-tunnel` exists but was **not** running in this sample.

Specific public IP values are omitted here (operational identifiers); region and ASN are the durable facts.

IMDS — Confirmed blocked

`http://169.254.169.254/` and IMDSv2 token PUT both **TCP time out** (~3 s). Route exists via the default gateway, but no service response — effective IMDS blackhole. Fail mode is timeout, not ICMP reject or HTTP 401.

Listening services (summary)

exec-daemon `:1337` / `:1338`, sand-host `:1340`, window-router, per-window helpers, localhost VNC/noVNC, localhost Chrome CDP, and `:2375` as noted above. Several helper ports lack user-visible process names in `ss`.

---

7. Software versions

Component	Version (CONFIRMED)
Base OS	Debian GNU/Linux **13 (trixie)** · `DEBIAN_VERSION_FULL=13.6`
Kernel	**6.12.94+**
Google Chrome	**151.0.7922.71**
Python 3	**3.13.5**
Node (distro `/usr/bin`)	**20.19.2**
Node (exec-daemon bundle)	**22.14.0**
bun	**1.3.14**
uv	**0.12.3**
git	2.47.3
ffmpeg	7.1.5
poppler (`pdftotext`)	25.03.0
gcc	14.2.0 (present); **make** not installed
tini	0.19.0
noVNC	1.6.0
xfwm4 / picom / Xvfb	4.20.0 / 12.5 / Xorg 21.1.16 stack
LibreOffice	**Not installed**
Timezone (machine)	**Etc/UTC** (user-facing zone Europe/Brussels)

8. Security and permissions

Identity and capabilities — Confirmed

Control	Observation
Default user	**box (uid 1000)** — not root for agent shells (SAND_USER_NON_ROOT=1)
Effective capabilities	**CapEff / CapPrm / CapInh = 0** (bounding set wide, effective empty)
Seccomp (sampled agent shell)	Off (Seccomp: 0, filters 0)
NoNewPrivs	0
AppArmor / SELinux	Tools absent; no in-box evidence of enforcing profiles
KASLR	Disabled in this guest
dmesg / kptrs	dmesg_restrict=0, kptr_restrict=0 (dmesg readable)
Kernel modules	Loading disabled (nomodule)
Swap	None
IMDS	Unreachable (timeout)
SSH agent forwarding path	vsock port 52 + /run/host-services/ssh-auth.sock (presence confirmed)

Privilege elevation and package installs — Confirmed (2026-08-12 recheck)

Fact	Result
Passwordless sudo -n	Works for user box
System apt with sudo	Can install system apt packages with sudo
apt without sudo	Fails; /usr not writable by box
User-space installs	uv, npm, bun
pip --user	Blocked by PEP 668

Practical implication: agents are non-root by default with cleared effective capabilities, but passwordless sudo provides a deliberate path to system package installation. Prefer uv / npm / bun for language tooling when possible; use sudo apt only when a system package is required.

Secrets policy for this summary

No API keys, tokens, cookies, private keys, or Authorization headers. Env IDs noted by name/length only (SAND_BOX_BOOT_ID, SAND_BOX_AUTH_ID, SAND_BOX_TENANT_ID,

SAND_BOX_STORE_ID). Files under sand-data secrets patterns listed by name only — contents not opened.

---

9. Unknowns

1. Exact AWS substrate under Firecracker (metal host / control-plane product details).
2. Whether `:2375` is a live Docker Engine or a shim.
3. Full PCI inventory (`lspci` absent; virtio sysfs only).
4. Physical host CPU SKU / NUMA (guest sees sanitized view).
5. SNAT pool size, hashing key, and whether `sand-egress-tunnel` ever becomes default egress when gated on.
6. Host network policy beyond the IMDS timeout (`iptables` / `nft` not usefully available from the box).
7. Persistence backend for `SAND_BOX_STORE_BACKEND=v2` (store type, region, encryption).
8. Seccomp posture of privileged services (only agent shell sampled).
9. Whether advertised nested `vmx` is usable (not tested).
10. Image channel (production vs canary) for kernel / Chrome / `sand-host` revisions.

---

10. One-line takeaway

A **Debian 13 agent runtime inside a Firecracker-on-KVM microVM**, with Docker overlay rootfs, multi-window X11 desktops, AWS us-west-2 SNAT egress, IMDS blackholed, non-root `box` (CapEff=0) plus **passwordless sudo for apt**, and user-space installs via **uv / npm / bun**.

Sources: live inspection of the agent computer on 2026-08-12