

Avoiding Crypto Miners from Hijacking your Kubernetes Cluster

Pre RKE we used Rancher 1.6. If you did not immediately lock down your cluster access using RBAC - your cluster would be saturated within 24 hours - assuming you are running directly on a public facing VPC.

```
ubuntu@a-osn-cd:~$ sudo ps -ef | grep stratum
ubuntu  24878 65468  0 15:36 pts/2    00:00:00 grep --color=auto stratum
root    60682 59879  0 Oct30 pts/1    00:00:00 /bin/sh -c ./xmrig -o stratum+tcp://monerohash.com:3333 -u
42kVTL3bciSHwjfJUNPif2JVMu4daFs6LVyBVtN9JbMXjLu6qZvwGtVJBF4PCeRHbZUiQDzBRBMu731EQWUHYGSoFz2r9fj -p x --max-cpu-
usage=100
root    61061 60682 99 Oct30 pts/1    34-08:13:23 ./xmrig -o stratum+tcp://monerohash.com:3333 -u
42kVTL3bciSHwjfJUNPif2JVMu4daFs6LVyBVtN9JbMXjLu6qZvwGtVJBF4PCeRHbZUiQDzBRBMu731EQWUHYGSoFz2r9fj -p x --max-cpu-
usage=100

  PID USER      PR  NI   VIRT   RES    SHR  S  %CPU  %MEM    TIME+
COMMAND
61061 root        20   0 4145488 145424  7500  S  4385  0.0  49449:50 ./xmrig -o stratum+tcp://monerohash.com:
3333 -u 42kVTL3bciSHwjfJUNPif2JVMu4daFs6LVyBVtN9JbMXjLu6qZvwGtVJBF4PCeRHbZUiQDzBRBMu731EQWUHYGSoFz2r9fj -p x+
```