1. 问题描述 1

客户EKS集群Kube-Proxy版本是kube-proxy:v1.21.2-eksbuild.2，控制平面是1.25，数据平面是1.24。升级VPC-CNI报如下错误：



1. Action 1

建议客户在升级add-on时选择Override，但是引入了另外一个问题。

1. 问题描述 2

通过Override升级后，客户的12个节点中，只有6个VPC-CNI节点是正常的，剩下6个VPC-CNI节点不正常。

1. Action 2

* 查看了aws node pod的日志，有ipamd进程异常报错。
* 通过命令查看了ipamd的日志，有如下错误：

kubectl exec -it aws-node-9cwkd -n kube-system -- /bin/bash cat /host/var/log/aws-routed-eni/ipamd.log

{"level":"error","ts":"2023-07-14T10:24:47.273Z","caller":"wait/wait.go:211","msg":"Unable to reach API Server, Get \"https://10.168.0.1:443/version?timeout=5s\": net/http: request canceled while waiting for connection (Client.Timeout exceeded while awaiting headers)"}

* 报错显示无法同API Server通信，于是查看了安全组，显示无异常
* 登录到aws node pod执行curl -k https://10.168.0.1:443/version?timeout=5s命令。其中异常aws node pod超时，正常aws node pod可以正常返回。
* 进一步查看iptables规则，发现异常aws node pod所在节点并未产生正确的iptables规则。
* 在网上找到了一篇行为一致的文章，解释了原因并给出了解决方案： [(1) Workloads unscheduleable after EKS 1.24 -> 1.25 upgrade : kubernetes (reddit.com)](https://www.reddit.com/r/kubernetes/comments/13wjsf3/workloads_unscheduleable_after_eks_124_125_upgrade/)。原因是控制平面升级到1.25后，1.21版本的kube proxy所使用的API版本被移除，导致kube-proxy无法创建iptables规则，进而影响了aws node pod和API Server的通信。
* 升级了kube proxy pod，重建了aws node pod，问题得到解决。