* Per far fronte alla vulnerabilità segnalata Sicurezza CAGS richiede come requisito di bloccare le porte oltre che su configurazioni di sistemi esterni (Firewall) - già applicate - anche su altro layer di protezione, esprimendo la necessità di utilizzare IPTABLES.
* Durante l'incontro RH segnala che:
  + Le uniche porte non autenticate in fase di installazione del Cluster sono 22623 e 22624. E blindandole si limita la scalabilità del cluster. Le porte in questione servono solo per la scalabilità del Cluster per aggiungere nuovi nodi o eliminarli. Se si utilizza DENY puntuali perdi funzionalità del Cluster.
  + Ad oggi non è previsto da documentazione ufficiale il blocco delle porte.

<https://docs.openshift.com/container-platform/4.14/post_installation_configuration/machine-configuration-tasks.html>

*Riporto estratto:*

*Currently, there is no supported way to block or restrict the machine config server endpoint.*

* IPTABLES non può essere applicato manualmente sui nodi del Cluster Openshift perché non è fattibile in quanto qualsiasi nodo OCP è un oggetto immutabile che può essere configurato solo dal prodotto.
* Eventualmente, per quanto esposto al punto precedente, può essere utilizzato un Operator con funzionalità like IPTABLES - *Node Firewall Operator* - con delle rule di configurazione. Questa strada fa riferimento ad uno scenario non ancora testato e certificato a livello di documentazione.

<https://docs.openshift.com/container-platform/4.14/networking/ingress-node-firewall-operator.html>

* È stato aggiornato il case 03859613 per far certificare la soluzione e comprenderne i rischi effettivi.

\*\*\* CASE \*\*\*

Sarebbe possibile oltre a quanto già effettuato sui firewall presenti al di fuori del cluster, limitare ai soli IP utili allo scale in / scale out, del cluster le porte 22623 e 22624 tramite una configurazione OpenShift? ad esempio utilizzando il Node Firewall Operator? Una soluzione simile può essere supportata? Quali sono i constrain o eventuali rischi?

Abbiamo la necessità di securizzare il più possibile il prodotto, in quanto al momento l'esposizione di queste 2 porte espone una vulnerability di sicurezza.

<https://docs.openshift.com/container-platform/4.14/networking/ingress-node-firewall-operator.html>