NeuVector

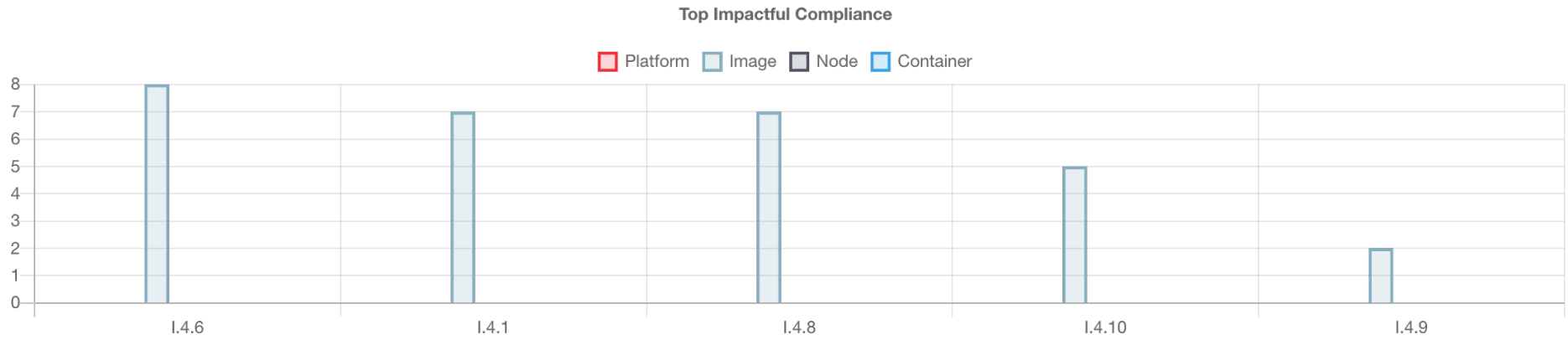
Full Lifecycle Container Security

Compliance Reports (Compliance View)

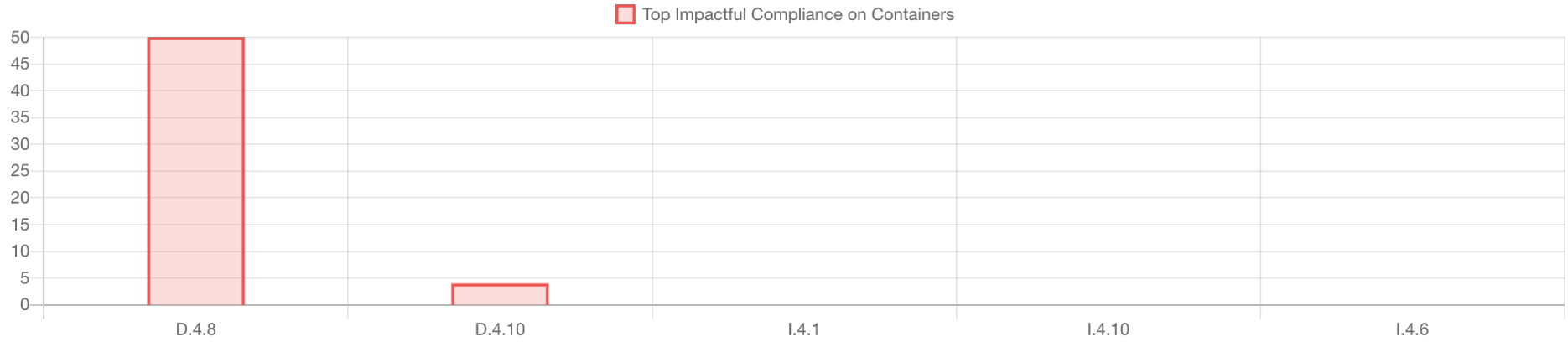
In this complianceList Report

Summary (Analyzed 19 records)

Top Impactful Compliance



Top Impactful Compliance on Containers



Details

Category	Name	Description	Level	Scored	Profile	Impact	remediation
docker	D.4.10	Ensure secrets are not stored in Dockerfiles - File /etc/ssh/ssh_host_dsa_key contains Private.Key: -----BEGIN DSA PRIVATE KEY--...	WARN	false	Level 1	**Containers** • nginx-pod-b965fcc45-gdb4p • node-pod-65fd6ddcb6-cxmxm • node-pod-65fd6ddcb6-qmszw • node-pod-65fd6ddcb6-wft6d	N/A
docker	D.4.8	Ensure setuid and setgid permissions are removed - File /var/local has setgid mode: dgrwxrwxr-x	WARN	false	Level 2	**Containers** • event-exporter-gke-5479fd58c8-dktkd • event-exporter-gke-5479fd58c8-dktkd • fluentbit-gke-6nc87 • fluentbit-gke-6nc87 • fluentbit-gke-cfn4g • .....(50 containers)	N/A
image	I.4.1	Ensure a user for the container has been created	WARN	true	Level 1	**Images** • nvbeta/api_server:latest • nvbeta/dns_client2:latest • nvbeta/exploit_1_21:latest • nvbeta/hello-world:latest • nvbeta/iodine:latest • .....(7 images)	N/A
image	I.4.10	Ensure secrets are not stored in container images - File /build/insecure_key.ppk contains Private.Key: PuTTY-User-Key-File...	WARN	false	Level 1	**Images** • nvbeta/dns_client2:latest • nvbeta/exploit_1_21:latest • nvbeta/nginx:latest • nvbeta/node:latest • nvbeta/swarm_nginx:latest	Please remove the file if it is not necessary
image	I.4.6	Ensure that HEALTHCHECK instructions have been added to container images	WARN	false	Level 1	**Images** • nvbeta/api_server:latest • nvbeta/dns_client2:latest • nvbeta/exploit_1_21:latest • nvbeta/hello-world:latest • nvbeta/iodine:latest • .....(8 images)	N/A
image	I.4.8	Ensure setuid and setgid permissions are removed - File /usr/local/lib/python3.4 has setgid mode: dgrwxrwxr-x	WARN	false	Level 2	**Images** • nvbeta/api_server:latest • nvbeta/dns_client2:latest • nvbeta/exploit_1_21:latest • nvbeta/iodine:latest • nvbeta/nginx:latest • .....(7 images)	N/A
image	I.4.9	Ensure that COPY is used instead of ADD in Dockerfiles	WARN	false	Level 1	**Images** • nvbeta/dns_client2:latest • nvbeta/node:latest	N/A
kubernetes	K.4.1.10	Ensure that the kubelet configuration file ownership is set to root:root - Wrong ownership for --config /home/kubernetes/kubelet-config.yaml	WARN	true	Level 1	**Nodes** • gke-cluster-1-default-pool-d051acb1-5z3m • gke-cluster-1-default-pool-d051acb1-9mr2 • gke-cluster-1-default-pool-d051acb1-k0qs • gke-cluster-1-default-pool-d051acb1-r9l9 • gke-cluster-1-default-pool-d051acb1-tztv	Run the following command (using the config file location identied in the Audit step) chown root:root /etc/kubernetes/kubelet.conf

Category	Name	Description	Level	Scored	Profile	Impact	remediation
kubernetes	K.4.1.9	Ensure that the kubelet configuration file has permissions set to 644 or more restrictive - Wrong permissions for --config / home/kubernetes/kubelet-config.yaml	WARN	true	Level 1	**Nodes** • gke-cluster-1-default-pool-d051acb1-5z3m • gke-cluster-1-default-pool-d051acb1-9mr2 • gke-cluster-1-default-pool-d051acb1-k0qs • gke-cluster-1-default-pool-d051acb1-r9l9 • gke-cluster-1-default-pool-d051acb1-tztv	Run the following command (using the config file location identied in the Audit step) chmod 644 / var/lib/kubelet/config.yaml
kubernetes	K.4.2.1	Ensure that the anonymous-auth argument is set to false	WARN	true	Level 1	**Nodes** • gke-cluster-1-default-pool-d051acb1-5z3m • gke-cluster-1-default-pool-d051acb1-9mr2 • gke-cluster-1-default-pool-d051acb1-k0qs • gke-cluster-1-default-pool-d051acb1-r9l9 • gke-cluster-1-default-pool-d051acb1-tztv	If using a Kubelet config file, edit the file to set authentication: anonymous: enabled to false. If using executable arguments, edit the kubelet service file /etc/systemd/system/ kubelet.service.d/10-kubeadm.conf on each worker node and set the below parameter in KUBELET_SYSTEM_PODS_ARGS variable. --anonymous-auth=false Based on your system, restart the kubelet service. For example: systemctl daemon-reload systemctl restart kubelet.service
kubernetes	K.4.2.10	Ensure that the --tls-cert-file and --tls-private-key-file arguments are set as appropriate	WARN	true	Level 1	**Nodes** • gke-cluster-1-default-pool-d051acb1-5z3m • gke-cluster-1-default-pool-d051acb1-9mr2 • gke-cluster-1-default-pool-d051acb1-k0qs • gke-cluster-1-default-pool-d051acb1-r9l9 • gke-cluster-1-default-pool-d051acb1-tztv	If using a Kubelet config file, edit the file to set tlsCertFile to the location of the certificate file to use to identify this Kubelet, and tlsPrivateKeyFile to the location of the corresponding private key file. If using command line arguments, edit the kubelet service file /etc/systemd/system/ kubelet.service.d/10-kubeadm.conf on each worker node and set the below parameters in KUBELET_CERTIFICATE_ARGS variable. --tls-cert-file=<path/to/tls-certificate-file> --tls-private-key-file=<path/to/tls-key-file> Based on your system, restart the kubelet service. For example: systemctl daemon-reload systemctl restart kubelet.service
kubernetes	K.4.2.11	Ensure that the --rotate-certificates argument is not set to false	WARN	true	Level 1	**Nodes** • gke-cluster-1-default-pool-d051acb1-5z3m • gke-cluster-1-default-pool-d051acb1-9mr2 • gke-cluster-1-default-pool-d051acb1-k0qs • gke-cluster-1-default-pool-d051acb1-r9l9 • gke-cluster-1-default-pool-d051acb1-tztv	If using a Kubelet config file, edit the file to add the line rotateCertificates: true or remove it altogether to use the default value. If using command line arguments, edit the kubelet service file /etc/systemd/system/kubelet.service.d/10-kubeadm.conf on each worker node and remove --rotate-certificates=false argument from the KUBELET_CERTIFICATE_ARGS variable. Based on your system, restart the kubelet service. For example: systemctl daemon-reload systemctl restart kubelet.service
kubernetes	K.4.2.12	Ensure that the RotateKubeletServerCertificate argument is set to true	WARN	true	Level 1	**Nodes** • gke-cluster-1-default-pool-d051acb1-5z3m • gke-cluster-1-default-pool-d051acb1-9mr2 • gke-cluster-1-default-pool-d051acb1-k0qs • gke-cluster-1-default-pool-d051acb1-r9l9 • gke-cluster-1-default-pool-d051acb1-tztv	On the master edit /var/lib/kubelet/kubeadm-flags.env and set the parameter KUBELET_CERTIFICATE_ARGS --feature-gates=RotateKubeletServerCertificate=true or as an alternative, and suggested as a last resort, edit the kubelet service file /etc/systemd/system/ kubelet.service.d/10-kubeadm.conf on each worker node and set the below parameter in KUBELET_CERTIFICATE_ARGS variable. --feature-gates=RotateKubeletServerCertificate=true Based on your system, restart the kubelet service. For example: systemctl daemon-reload systemctl restart kubelet.service

Category	Name	Description	Level	Scored	Profile	Impact	remediation
kubernetes	K.4.2.13	Ensure that the Kubelet only makes use of Strong Cryptographic Ciphers	WARN	false	Level 1	**Nodes** • gke-cluster-1-default-pool-d051acb1-5z3m • gke-cluster-1-default-pool-d051acb1-9mr2 • gke-cluster-1-default-pool-d051acb1-k0qs • gke-cluster-1-default-pool-d051acb1-r9l9 • gke-cluster-1-default-pool-d051acb1-tztv	If using a Kubelet config file, edit the file to set TLSCipherSuites: to TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256,TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 ,TLS_ECDHE_ECDSA_WITH_CHACHA20_POLY1305,TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 ,TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305,TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384,TLS_RSA_WITH_AES_256_GCM_SHA384,TLS_RSA_WITH_AES_128_GCM_SHA256 or to a subset of these values. If using executable arguments, edit the kubelet service file /etc/systemd/system/kubelet.service.d/10-kubeadm.conf on each worker node and set the --tls-cipher-suites parameter as follows, or to a subset of these values. --tls-cipher-suites=TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256,TLS_ECDHE_RSA_WITH_AES_128_GCM _SHA256,TLS_ECDHE_ECDSA_WITH_CHACHA20_POLY1305,TLS_ECDHE_RSA_WITH_AES_256_GCM _SHA384,TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305,TLS_ECDHE_ECDSA_WITH_AES_256_GCM _SHA384,TLS_RSA_WITH_AES_256_GCM_SHA384,TLS_RSA_WITH_AES_128_GCM_SHA256 Based on your system, restart the kubelet service. For example: systemctl daemon-reload systemctl restart kubelet.service
kubernetes	K.4.2.3	Ensure that the --client-ca-file argument is set as appropriate	WARN	true	Level 1	**Nodes** • gke-cluster-1-default-pool-d051acb1-5z3m • gke-cluster-1-default-pool-d051acb1-9mr2 • gke-cluster-1-default-pool-d051acb1-k0qs • gke-cluster-1-default-pool-d051acb1-r9l9 • gke-cluster-1-default-pool-d051acb1-tztv	If using a Kubelet config file, edit the file to set authentication: x509: clientCAFile to the location of the client CA file. If using command line arguments, edit the kubelet service file /etc/systemd/system/kubelet.service.d/10-kubeadm.conf on each worker node and set the below parameter in KUBELET_AUTHZ_ARGS variable. --client-ca-file=<path/to/client-ca-file> Based on your system, restart the kubelet service. For example: systemctl daemon-reload systemctl restart kubelet.service
kubernetes	K.4.2.4	Ensure that the --read-only-port argument is set to 0	WARN	true	Level 1	**Nodes** • gke-cluster-1-default-pool-d051acb1-5z3m • gke-cluster-1-default-pool-d051acb1-9mr2 • gke-cluster-1-default-pool-d051acb1-k0qs • gke-cluster-1-default-pool-d051acb1-r9l9 • gke-cluster-1-default-pool-d051acb1-tztv	If using a Kubelet config file, edit the file to set readOnlyPort to 0. If using command line arguments, edit the kubelet service file /etc/systemd/system/kubelet.service.d/10-kubeadm.conf on each worker node and set the below parameter in KUBELET_SYSTEM_PODS_ARGS variable. --read-only-port=0 Based on your system, restart the kubelet service. For example: systemctl daemon-reload systemctl restart kubelet.service

Category	Name	Description	Level	Scored	Profile	Impact	remediation
kubernetes	K.4.2.6	Ensure that the --protect-kernel-defaults argument is set to true	WARN	true	Level 1	**Nodes** • gke-cluster-1-default-pool-d051acb1-5z3m • gke-cluster-1-default-pool-d051acb1-9mr2 • gke-cluster-1-default-pool-d051acb1-k0qs • gke-cluster-1-default-pool-d051acb1-r9l9 • gke-cluster-1-default-pool-d051acb1-tztv	If using a Kubelet config file, edit the file to set protectKernelDefaults: true. If using command line arguments, edit the kubelet service file /etc/systemd/system/kubelet.service.d/10-kubeadm.conf on each worker node and set the below parameter in KUBELET_SYSTEM_PODS_ARGS variable. --protect-kernel-defaults=true Based on your system, restart the kubelet service. For example: systemctl daemon-reload systemctl restart kubelet.service
kubernetes	K.4.2.7	Ensure that the --make-iptables-util-chains argument is set to true	WARN	true	Level 1	**Nodes** • gke-cluster-1-default-pool-d051acb1-5z3m • gke-cluster-1-default-pool-d051acb1-9mr2 • gke-cluster-1-default-pool-d051acb1-k0qs • gke-cluster-1-default-pool-d051acb1-r9l9 • gke-cluster-1-default-pool-d051acb1-tztv	If using a Kubelet config file, edit the file to set makeIPTablesUtilChains: true. If using command line arguments, edit the kubelet service file /etc/systemd/system/kubelet.service.d/10-kubeadm.conf on each worker node and remove the --make-iptables-util-chains argument from the KUBELET_SYSTEM_PODS_ARGS variable. Based on your system, restart the kubelet service. For example: systemctl daemon-reload systemctl restart kubelet.service
kubernetes	K.4.2.9	Ensure that the --event-qps argument is set to 0 or a level which ensures appropriate event capture	WARN	false	Level 2	**Nodes** • gke-cluster-1-default-pool-d051acb1-5z3m • gke-cluster-1-default-pool-d051acb1-9mr2 • gke-cluster-1-default-pool-d051acb1-k0qs • gke-cluster-1-default-pool-d051acb1-r9l9 • gke-cluster-1-default-pool-d051acb1-tztv	If using a Kubelet config file, edit the file to set eventRecordQPS: to an appropriate level. If using command line arguments, edit the kubelet service file /etc/systemd/system/kubelet.service.d/10-kubeadm.conf on each worker node and set the below parameter in KUBELET_SYSTEM_PODS_ARGS variable. Based on your system, restart the kubelet service. For example: systemctl daemon-reload systemctl restart kubelet.service

Appendix (Full impact list) (Show full list of images, containers, nodes and platforms)

D.4.10

Containers: 4

nginx-pod-b965fcc45-gdb4p
node-pod-65fd6ddcb6-cxmxm
node-pod-65fd6ddcb6-qmszw
node-pod-65fd6ddcb6-wft6d

D.4.8

Containers: 50

event-exporter-gke-5479fd58c8-dktkd
event-exporter-gke-5479fd58c8-dktkd
fluentbit-gke-6nc87
fluentbit-gke-6nc87
fluentbit-gke-cfn4g
fluentbit-gke-cfn4g
fluentbit-gke-ljrgv
fluentbit-gke-ljrgv
fluentbit-gke-tm92t
fluentbit-gke-tm92t
fluentbit-gke-zx587
fluentbit-gke-zx587
gke-metrics-agent-4h522
gke-metrics-agent-mrlvl
gke-metrics-agent-n7ttl
gke-metrics-agent-p4zv8
gke-metrics-agent-r4jh9
konnectivity-agent-autoscaler-5c49cb58bb-zv88w
kube-dns-697dc8fc8b-c9mrq
kube-dns-697dc8fc8b-c9mrq
kube-dns-697dc8fc8b-c9mrq
kube-dns-697dc8fc8b-c9mrq
kube-dns-697dc8fc8b-kkvk9
kube-dns-697dc8fc8b-kkvk9
kube-dns-697dc8fc8b-kkvk9
kube-dns-autoscaler-844c9d9448-f5jlz
kube-proxy-gke-cluster-1-default-pool-d051acb1-5z3m
kube-proxy-gke-cluster-1-default-pool-d051acb1-9mr2
kube-proxy-gke-cluster-1-default-pool-d051acb1-k0qs
kube-proxy-gke-cluster-1-default-pool-d051acb1-r9l9
kube-proxy-gke-cluster-1-default-pool-d051acb1-tztv
l7-default-backend-69fb9fd9f9-7fdjj
metrics-server-v0.4.4-857776bc9c-bfhbp
metrics-server-v0.4.4-857776bc9c-bfhbp
nginx-pod-b965fcc45-gdb4p
node-pod-65fd6ddcb6-cxmxm
node-pod-65fd6ddcb6-qmszw
node-pod-65fd6ddcb6-wft6d
pdcsi-node-2vpps
pdcsi-node-2vpps
pdcsi-node-4fhgs
pdcsi-node-4fhgs
pdcsi-node-8sfmp
pdcsi-node-8sfmp
pdcsi-node-9s9js
pdcsi-node-9s9js
pdcsi-node-mnzct
pdcsi-node-mnzct
redis-pod-65c9cb584b-969tn

I.4.1

Images: 7

nvbeta/api_server:latest
nvbeta/dns_client2:latest
nvbeta/exploit_1_21:latest
nvbeta/hello-world:latest
nvbeta/iodine:latest
nvbeta/nginx:latest
nvbeta/swarm_nginx:latest

I.4.10

Images: 5

nvbeta/dns_client2:latest
nvbeta/exploit_1_21:latest
nvbeta/nginx:latest

nvbeta/node:latest
nvbeta/swarm_nginx:latest

I.4.6

Images: 8

nvbeta/api_server:latest
nvbeta/dns_client2:latest
nvbeta/exploit_1_21:latest
nvbeta/hello-world:latest
nvbeta/iodine:latest
nvbeta/nginx:latest
nvbeta/node:latest
nvbeta/swarm_nginx:latest

I.4.8

Images: 7

nvbeta/api_server:latest
nvbeta/dns_client2:latest
nvbeta/exploit_1_21:latest
nvbeta/iodine:latest
nvbeta/nginx:latest
nvbeta/node:latest
nvbeta/swarm_nginx:latest

I.4.9

Images: 2

nvbeta/dns_client2:latest
nvbeta/node:latest

K.4.1.10

Nodes: 5

gke-cluster-1-default-pool-d051acb1-5z3m
gke-cluster-1-default-pool-d051acb1-9mr2
gke-cluster-1-default-pool-d051acb1-k0qs
gke-cluster-1-default-pool-d051acb1-r9l9
gke-cluster-1-default-pool-d051acb1-tztv

K.4.1.9

Nodes: 5

gke-cluster-1-default-pool-d051acb1-5z3m
gke-cluster-1-default-pool-d051acb1-9mr2
gke-cluster-1-default-pool-d051acb1-k0qs
gke-cluster-1-default-pool-d051acb1-r9l9
gke-cluster-1-default-pool-d051acb1-tztv

K.4.2.1

Nodes: 5

gke-cluster-1-default-pool-d051acb1-5z3m
gke-cluster-1-default-pool-d051acb1-9mr2
gke-cluster-1-default-pool-d051acb1-k0qs
gke-cluster-1-default-pool-d051acb1-r9l9
gke-cluster-1-default-pool-d051acb1-tztv

K.4.2.10

Nodes: 5

gke-cluster-1-default-pool-d051acb1-5z3m
gke-cluster-1-default-pool-d051acb1-9mr2
gke-cluster-1-default-pool-d051acb1-k0qs
gke-cluster-1-default-pool-d051acb1-r9l9
gke-cluster-1-default-pool-d051acb1-tztv

K.4.2.11

Nodes: 5

gke-cluster-1-default-pool-d051acb1-5z3m
gke-cluster-1-default-pool-d051acb1-9mr2
gke-cluster-1-default-pool-d051acb1-k0qs
gke-cluster-1-default-pool-d051acb1-r9l9
gke-cluster-1-default-pool-d051acb1-tztv

K.4.2.12

Nodes: 5

gke-cluster-1-default-pool-d051acb1-5z3m
gke-cluster-1-default-pool-d051acb1-9mr2
gke-cluster-1-default-pool-d051acb1-k0qs
gke-cluster-1-default-pool-d051acb1-r9l9
gke-cluster-1-default-pool-d051acb1-tztv

K.4.2.13

Nodes: 5

gke-cluster-1-default-pool-d051acb1-5z3m
gke-cluster-1-default-pool-d051acb1-9mr2
gke-cluster-1-default-pool-d051acb1-k0qs
gke-cluster-1-default-pool-d051acb1-r9l9
gke-cluster-1-default-pool-d051acb1-tztv

K.4.2.3

Nodes: 5

gke-cluster-1-default-pool-d051acb1-5z3m
gke-cluster-1-default-pool-d051acb1-9mr2
gke-cluster-1-default-pool-d051acb1-k0qs
gke-cluster-1-default-pool-d051acb1-r9l9
gke-cluster-1-default-pool-d051acb1-tztv

K.4.2.4

Nodes: 5

gke-cluster-1-default-pool-d051acb1-5z3m
gke-cluster-1-default-pool-d051acb1-9mr2
gke-cluster-1-default-pool-d051acb1-k0qs
gke-cluster-1-default-pool-d051acb1-r9l9
gke-cluster-1-default-pool-d051acb1-tztv

K.4.2.6

Nodes: 5

gke-cluster-1-default-pool-d051acb1-5z3m
gke-cluster-1-default-pool-d051acb1-9mr2
gke-cluster-1-default-pool-d051acb1-k0qs
gke-cluster-1-default-pool-d051acb1-r9l9
gke-cluster-1-default-pool-d051acb1-tztv

K.4.2.7

Nodes: 5

gke-cluster-1-default-pool-d051acb1-5z3m
gke-cluster-1-default-pool-d051acb1-9mr2
gke-cluster-1-default-pool-d051acb1-k0qs
gke-cluster-1-default-pool-d051acb1-r9l9
gke-cluster-1-default-pool-d051acb1-tztv

K.4.2.9

Nodes: 5

gke-cluster-1-default-pool-d051acb1-5z3m
gke-cluster-1-default-pool-d051acb1-9mr2
gke-cluster-1-default-pool-d051acb1-k0qs
gke-cluster-1-default-pool-d051acb1-r9l9
gke-cluster-1-default-pool-d051acb1-tztv