NeuVector

Full Lifecycle Container Security

Compliance Reports (Assets View)

Full Compliance Report (Assets View)

Details (Please refer appendix for details of compliance)

Containers (Compliant Workloads (No Compliance Violations): 47% (44 Workload(s)))

Name	Namespace	Applications	Policy Mode	Group	Compliance Count	Compliance List	Scanned at
nginx-pod-b965fcc45-gdb4p	demo	nginx	Protect	nv.nginx-pod.demo	2	D.4.10 D.4.8	
node-pod-65fd6ddcb6-cxmxm	demo	TCP/8888	Protect	nv.node-pod.demo	2	D.4.10 D.4.8	Feb 17, 2022 15:26:22
node-pod-65fd6ddcb6-qmszw	demo		Protect	nv.node-pod.demo	2	D.4.10 D.4.8	Feb 17, 2022 15:07:13
node-pod-65fd6ddcb6-wft6d	demo	TCP/8888	Protect	nv.node-pod.demo	2	D.4.10 D.4.8	Feb 17, 2022 15:40:53
event-exporter-gke-5479fd58c8-dktkd	kube-system	TCP/8080, TCP/16061, TCP/6061	Protect	nv.event-exporter-gke.kube-system	1	D.4.8	Feb 17, 2022 06:35:29
event-exporter-gke-5479fd58c8-dktkd	kube-system	TCP/8080, TCP/16061, TCP/6061	Protect	nv.event-exporter-gke.kube-system	1	D.4.8	Feb 17, 2022 06:35:29
fluentbit-gke-6nc87	kube-system	TCP/2021, TCP/2020	Protect	nv.fluentbit-gke.kube-system	1	D.4.8	Feb 17, 2022 06:35:05
fluentbit-gke-6nc87	kube-system	TCP/2021, TCP/2020	Protect	nv.fluentbit-gke.kube-system	1	D.4.8	Feb 17, 2022 06:35:05
fluentbit-gke-cfn4g	kube-system	TCP/2020, TCP/2021	Protect	nv.fluentbit-gke.kube-system	1	D.4.8	Feb 17, 2022 06:34:38
fluentbit-gke-cfn4g	kube-system	TCP/2020, TCP/2021	Protect	nv.fluentbit-gke.kube-system	1	D.4.8	Feb 17, 2022 06:34:38
fluentbit-gke-ljrgv	kube-system	TCP/2020, TCP/2021	Protect	nv.fluentbit-gke.kube-system	1	D.4.8	Feb 17, 2022 06:35:29
fluentbit-gke-ljrgv	kube-system	TCP/2020, TCP/2021	Protect	nv.fluentbit-gke.kube-system	1	D.4.8	Feb 17, 2022 06:35:29
fluentbit-gke-tm92t	kube-system	TCP/2020, TCP/2021	Protect	nv.fluentbit-gke.kube-system	1	D.4.8	Feb 17, 2022 06:35:30
fluentbit-gke-tm92t	kube-system	TCP/2020, TCP/2021	Protect	nv.fluentbit-gke.kube-system	1	D.4.8	Feb 17, 2022 06:35:30
fluentbit-gke-zx587	kube-system	TCP/2020, TCP/2021	Protect	nv.fluentbit-gke.kube-system	1	D.4.8	Feb 17, 2022 06:34:37
fluentbit-gke-zx587	kube-system	TCP/2020, TCP/2021	Protect	nv.fluentbit-gke.kube-system	1	D.4.8	Feb 17, 2022

Name	Namespace	Applications	Policy Mode	Group	Compliance Count	Compliance List	Scanned at
							06:34:37
gke-metrics-agent-4h522	kube-system	TCP/8200	Protect	nv.gke-metrics-agent.kube-system	1	D.4.8	Feb 17, 2022 06:35:18
gke-metrics-agent-mrlvl	kube-system	TCP/8200	Protect	nv.gke-metrics-agent.kube-system	1	D.4.8	Feb 17, 2022 06:35:26
gke-metrics-agent-n7ttl	kube-system	TCP/8200	Protect	nv.gke-metrics-agent.kube-system	1	D.4.8	Feb 17, 2022 06:34:57
gke-metrics-agent-p4zv8	kube-system	TCP/8200	Protect	nv.gke-metrics-agent.kube-system	1	D.4.8	Feb 17, 2022 06:34:38
gke-metrics-agent-r4jh9	kube-system	TCP/8200	Protect	nv.gke-metrics-agent.kube-system	1	D.4.8	Feb 17, 2022 06:35:02
konnectivity-agent-autoscaler-5c49cb58bb-zv88w	kube-system	TCP/8080	Protect	nv.konnectivity-agent-autoscaler.kube-system	1	D.4.8	Feb 17, 2022 06:34:38
kube-dns-697dc8fc8b-c9mrq	kube-system	TCP/10055, TCP/53, TCP/6061, HTTP, UDP/10053, UDP/53, TCP/10053	Protect	nv.kube-dns.kube-system	1	D.4.8	Feb 17, 2022 06:34:53
kube-dns-697dc8fc8b-c9mrq	kube-system	TCP/10055, TCP/53, TCP/6061, HTTP, UDP/10053, UDP/53, TCP/10053	Protect	nv.kube-dns.kube-system	1	D.4.8	Feb 17, 2022 06:34:53
kube-dns-697dc8fc8b-c9mrq	kube-system	TCP/10055, TCP/53, TCP/6061, HTTP, UDP/10053, UDP/53, TCP/10053	Protect	nv.kube-dns.kube-system	1	D.4.8	Feb 17, 2022 06:34:53
kube-dns-697dc8fc8b-c9mrq	kube-system	TCP/10055, TCP/53, TCP/6061, HTTP, UDP/10053, UDP/53, TCP/10053	Protect	nv.kube-dns.kube-system	1	D.4.8	Feb 17, 2022 06:34:53
kube-dns-697dc8fc8b-kkvk9	kube-system	UDP/53, TCP/10053, HTTP, TCP/10055, TCP/53, TCP/6061, UDP/10053	Protect	nv.kube-dns.kube-system	1	D.4.8	Feb 17, 2022 06:34:35
kube-dns-697dc8fc8b-kkvk9	kube-system	UDP/53, TCP/10053, HTTP, TCP/10055, TCP/53, TCP/6061, UDP/10053	Protect	nv.kube-dns.kube-system	1	D.4.8	Feb 17, 2022 06:34:35
kube-dns-697dc8fc8b-kkvk9	kube-system	UDP/53, TCP/10053, HTTP, TCP/10055, TCP/53, TCP/6061, UDP/10053	Protect	nv.kube-dns.kube-system	1	D.4.8	Feb 17, 2022 06:34:35
kube-dns-697dc8fc8b-kkvk9	kube-system	UDP/53, TCP/10053, HTTP, TCP/10055, TCP/53, TCP/6061, UDP/10053	Protect	nv.kube-dns.kube-system	1	D.4.8	Feb 17, 2022 06:34:35
kube-dns-autoscaler-844c9d9448-f5jlz	kube-system	TCP/8080	Protect	nv.kube-dns-autoscaler.kube-system	1	D.4.8	Feb 17, 2022 06:35:05
kube-proxy-gke-cluster-1-default-pool-d051acb1-5z3m	kube-system	TCP/10256, TCP/30980, TCP/31579, TCP/32419,	Protect	nv.kube-proxy-gke-cluster-1-default-pool-	1	D.4.8	Feb 17, 2022

Name	Namespace	Applications	Policy Mode	Group	Compliance Count	Compliance List	Scanned at
		TCP/10249		d051acb1.kube-system			06:34:38
kube-proxy-gke-cluster-1-default-pool-d051acb1-9mr2	kube-system	TCP/31579, TCP/32419, TCP/10249, TCP/10256, TCP/30980	Protect	nv.kube-proxy-gke-cluster-1-default-pool-d051acb1.kube-system	1	D.4.8	Feb 17, 2022 06:35:19
kube-proxy-gke-cluster-1-default-pool-d051acb1-k0qs	kube-system	TCP/32419, TCP/10249, TCP/10256, TCP/30980, TCP/31579	Protect	nv.kube-proxy-gke-cluster-1-default-pool-d051acb1.kube-system	1	D.4.8	Feb 17, 2022 06:34:57
kube-proxy-gke-cluster-1-default-pool-d051acb1-r9l9	kube-system	TCP/31579, TCP/32419, TCP/10249, TCP/10256, TCP/30980	Protect	nv.kube-proxy-gke-cluster-1-default-pool-d051acb1.kube-system	1	D.4.8	Feb 17, 2022 06:35:26
kube-proxy-gke-cluster-1-default-pool-d051acb1-tztv	kube-system	TCP/30980, TCP/31579, TCP/32419, TCP/10249, TCP/10256	Protect	nv.kube-proxy-gke-cluster-1-default-pool-d051acb1.kube-system	1	D.4.8	Feb 17, 2022 06:34:45
l7-default-backend-69fb9fd9f9-7fdjj	kube-system	HTTP, TCP/8081	Protect	nv.l7-default-backend.kube-system	1	D.4.8	Feb 17, 2022 06:35:26
metrics-server-v0.4.4-857776bc9c-bfhbp	kube-system	SSL	Protect	nv.metrics-server-v0.4.4.kube-system	1	D.4.8	Feb 17, 2022 06:35:19
metrics-server-v0.4.4-857776bc9c-bfhbp	kube-system	SSL	Protect	nv.metrics-server-v0.4.4.kube-system	1	D.4.8	Feb 17, 2022 06:35:19
pdcsi-node-2vpps	kube-system		Protect	nv.pdcsi-node.kube-system	1	D.4.8	Feb 17, 2022 06:35:00
pdcsi-node-2vpps	kube-system		Protect	nv.pdcsi-node.kube-system	1	D.4.8	Feb 17, 2022 06:35:00
pdcsi-node-4fhgs	kube-system		Protect	nv.pdcsi-node.kube-system	1	D.4.8	Feb 17, 2022 06:35:26
pdcsi-node-4fhgs	kube-system		Protect	nv.pdcsi-node.kube-system	1	D.4.8	Feb 17, 2022 06:35:26
pdcsi-node-8sfmp	kube-system		Protect	nv.pdcsi-node.kube-system	1	D.4.8	Feb 17, 2022 06:35:26
pdcsi-node-8sfmp	kube-system		Protect	nv.pdcsi-node.kube-system	1	D.4.8	Feb 17, 2022 06:35:26
pdcsi-node-9s9js	kube-system		Protect	nv.pdcsi-node.kube-system	1	D.4.8	Feb 17, 2022 06:34:35
pdcsi-node-9s9js	kube-system		Protect	nv.pdcsi-node.kube-system	1	D.4.8	Feb 17, 2022 06:34:35
pdcsi-node-mnzct	kube-system		Protect	nv.pdcsi-node.kube-system	1	D.4.8	Feb 17, 2022

Name	Namespace	Applications	Policy Mode	Group	Compliance Count	Compliance List	Scanned at
							06:34:38
pdcsi-node-mnzct	kube-system		Protect	nv.pdcsi-node.kube-system	1	D.4.8	Feb 17, 2022 06:34:38
redis-pod-65c9cb584b-969tn	demo	Redis	Protect	nv.redis-pod.demo	1	D.4.8	Feb 17, 2022 15:01:31
event-exporter-gke-5479fd58c8-dktkd	kube-system	TCP/8080, TCP/16061, TCP/6061	Protect	nv.event-exporter-gke.kube-system	0		2022-02-17 T01:05:29Z
fluentbit-gke-6nc87	kube-system	TCP/2021, TCP/2020	Protect	nv.fluentbit-gke.kube-system	0		2022-02-17 T01:05:05Z
fluentbit-gke-cfn4g	kube-system	TCP/2020, TCP/2021	Protect	nv.fluentbit-gke.kube-system	0		2022-02-17 T01:04:38Z
fluentbit-gke-ljrgv	kube-system	TCP/2020, TCP/2021	Protect	nv.fluentbit-gke.kube-system	0		2022-02-17 T01:05:29Z
fluentbit-gke-tm92t	kube-system	TCP/2020, TCP/2021	Protect	nv.fluentbit-gke.kube-system	0		2022-02-17 T01:05:30Z
fluentbit-gke-zx587	kube-system	TCP/2020, TCP/2021	Protect	nv.fluentbit-gke.kube-system	0		2022-02-17 T01:04:37Z
gke-metrics-agent-4h522	kube-system	TCP/8200	Protect	nv.gke-metrics-agent.kube-system	0		2022-02-17 T01:05:18Z
gke-metrics-agent-mrlvl	kube-system	TCP/8200	Protect	nv.gke-metrics-agent.kube-system	0		2022-02-17 T01:05:26Z
gke-metrics-agent-n7ttl	kube-system	TCP/8200	Protect	nv.gke-metrics-agent.kube-system	0		2022-02-17 T01:04:57Z
gke-metrics-agent-p4zv8	kube-system	TCP/8200	Protect	nv.gke-metrics-agent.kube-system	0		2022-02-17 T01:04:38Z
gke-metrics-agent-r4jh9	kube-system	TCP/8200	Protect	nv.gke-metrics-agent.kube-system	0		2022-02-17 T01:05:02Z
konnectivity-agent-86678fb5f5-6j2xk	kube-system	HTTP, TCP/8094	Protect	nv.konnectivity-agent.kube-system	0		2022-02-17 T01:05:19Z
konnectivity-agent-86678fb5f5-6j2xk	kube-system	HTTP, TCP/8094	Protect	nv.konnectivity-agent.kube-system	0		Feb 17, 2022 06:35:19
konnectivity-agent-86678fb5f5-bhlfs	kube-system	HTTP, TCP/8094	Protect	nv.konnectivity-agent.kube-system	0		2022-02-17 T01:04:38Z
konnectivity-agent-86678fb5f5-bhlfs	kube-system	HTTP, TCP/8094	Protect	nv.konnectivity-agent.kube-system	0		Feb 17, 2022 06:34:38
konnectivity-agent-86678fb5f5-jb8v6	kube-system	HTTP, TCP/8094	Protect	nv.konnectivity-agent.kube-system	0		2022-02-17 T01:04:35Z
konnectivity-agent-86678fb5f5-jb8v6	kube-system	HTTP, TCP/8094	Protect	nv.konnectivity-agent.kube-system	0		Feb 17, 2022 06:34:35
konnectivity-agent-86678fb5f5-ksdst	kube-system	HTTP, TCP/8094	Protect	nv.konnectivity-agent.kube-system	0		2022-02-17 T01:05:18Z

Name	Namespace	Applications	Policy Mode	Group	Compliance Count	Compliance List	Scanned at
konnectivity-agent-86678fb5f5-ksdst	kube-system	HTTP, TCP/8094	Protect	nv.konnectivity-agent.kube-system	0		Feb 17, 2022 06:35:18
konnectivity-agent-86678fb5f5-w74kn	kube-system	TCP/8094, HTTP	Protect	nv.konnectivity-agent.kube-system	0		2022-02-17 T01:05:10Z
konnectivity-agent-86678fb5f5-w74kn	kube-system	TCP/8094, HTTP	Protect	nv.konnectivity-agent.kube-system	0		Feb 17, 2022 06:35:10
konnectivity-agent-autoscaler-5c49cb58bb-zv88w	kube-system	TCP/8080	Protect	nv.konnectivity-agent-autoscaler.kube-system	0		2022-02-17 T01:04:38Z
kube-dns-697dc8fc8b-c9mrq	kube-system	TCP/10055, TCP/53, TCP/6061, HTTP, UDP/10053, UDP/53, TCP/10053	Protect	nv.kube-dns.kube-system	0		2022-02-17 T01:04:53Z
kube-dns-697dc8fc8b-kkvk9	kube-system	UDP/53, TCP/10053, HTTP, TCP/10055, TCP/53, TCP/6061, UDP/10053	Protect	nv.kube-dns.kube-system	0		2022-02-17 T01:04:35Z
kube-dns-autoscaler-844c9d9448-f5jlz	kube-system	TCP/8080	Protect	nv.kube-dns-autoscaler.kube-system	0		2022-02-17 T01:05:05Z
kube-proxy-gke-cluster-1-default-pool-d051acb1-5z3m	kube-system	TCP/10256, TCP/30980, TCP/31579, TCP/32419, TCP/10249	Protect	nv.kube-proxy-gke-cluster-1-default-pool-d051acb1.kube-system	0		2022-02-17 T01:04:38Z
kube-proxy-gke-cluster-1-default-pool-d051acb1-9mr2	kube-system	TCP/31579, TCP/32419, TCP/10249, TCP/10256, TCP/30980	Protect	nv.kube-proxy-gke-cluster-1-default-pool-d051acb1.kube-system	0		2022-02-17 T01:05:19Z
kube-proxy-gke-cluster-1-default-pool-d051acb1-k0qs	kube-system	TCP/32419, TCP/10249, TCP/10256, TCP/30980, TCP/31579	Protect	nv.kube-proxy-gke-cluster-1-default-pool-d051acb1.kube-system	0		2022-02-17 T01:04:57Z
kube-proxy-gke-cluster-1-default-pool-d051acb1-r9l9	kube-system	TCP/31579, TCP/32419, TCP/10249, TCP/10256, TCP/30980	Protect	nv.kube-proxy-gke-cluster-1-default-pool-d051acb1.kube-system	0		2022-02-17 T01:05:26Z
kube-proxy-gke-cluster-1-default-pool-d051acb1-tztv	kube-system	TCP/30980, TCP/31579, TCP/32419, TCP/10249, TCP/10256	Protect	nv.kube-proxy-gke-cluster-1-default-pool-d051acb1.kube-system	0		2022-02-17 T01:04:45Z
l7-default-backend-69fb9fd9f9-7fdjj	kube-system	HTTP, TCP/8081	Protect	nv.l7-default-backend.kube-system	0		2022-02-17 T01:05:26Z
metrics-server-v0.4.4-857776bc9c-bfhbp	kube-system	SSL	Protect	nv.metrics-server-v0.4.4.kube-system	0		2022-02-17 T01:05:19Z
nginx-pod-b965fcc45-gdb4p	demo	nginx	Protect	nv.nginx-pod.demo	0		
node-pod-65fd6ddcb6-cxmxm	demo	TCP/8888	Protect	nv.node-pod.demo	0		2022-02-17 T09:56:22Z
node-pod-65fd6ddcb6-qmszw	demo		Protect	nv.node-pod.demo	0		2022-02-17 T09:37:13Z
node-pod-65fd6ddcb6-wft6d	demo	TCP/8888	Protect	nv.node-pod.demo	0		2022-02-17 T10:10:53Z
pdcsi-node-2vpps	kube-system		Protect	nv.pdcsi-node.kube-system	0		2022-02-17 T01:05:00Z

Name	Namespace	Applications	Policy Mode	Group	Compliance Count	Compliance List	Scanned at
pdcsi-node-4fhgs	kube-system		Protect	nv.pdcsi-node.kube-system	0		2022-02-17 T01:05:26Z
pdcsi-node-8sfmp	kube-system		Protect	nv.pdcsi-node.kube-system	0		2022-02-17 T01:05:26Z
pdcsi-node-9s9js	kube-system		Protect	nv.pdcsi-node.kube-system	0		2022-02-17 T01:04:35Z
pdcsi-node-mnzct	kube-system		Protect	nv.pdcsi-node.kube-system	0		2022-02-17 T01:04:38Z
redis-pod-65c9cb584b-969tn	demo	Redis	Protect	nv.redis-pod.demo	0		2022-02-17 T09:31:31Z
redis-pod-7bbd468657-jzzv4	demo		Protect	nv.redis-pod.demo	0		2022-02-17 T01:05:15Z
neuvector-updater-pod-27417600-x9pfb	neuvector		discover		0		

Hosts (Compliant Hosts (No Compliance Violations): 0% (0 Host(s)))

Name	OS	Kernel Version	CPUs	Memory	Containers	Policy Mode	Compliance Count	Compliance List	Scanned at
gke-cluster-1-default-pool-d051acb1-5z3m	Container-Optimized OS from Google	5.4.144+	2	4128243712	19	Protect	12	K.4.1.10 K.4.1.9 K.4.2.1 K.4.2.10 K.4.2.11 K.4.2.12 K.4.2.13 K.4.2.3 K.4.2.4 K.4.2.6 K.4.2.7 K.4.2.9	Feb 17, 2022 06:35:26
gke-cluster-1-default-pool-d051acb1-9mr2	Container-Optimized OS from Google	5.4.144+	2	4128243712	19	Protect	12	K.4.1.10 K.4.1.9 K.4.2.1 K.4.2.10 K.4.2.11 K.4.2.12 K.4.2.13 K.4.2.3 K.4.2.4 K.4.2.6 K.4.2.7 K.4.2.9	Feb 17, 2022 06:34:49
gke-cluster-1-default-pool-d051acb1-k0qs	Container-Optimized OS from Google	5.4.144+	2	4128243712	20	Protect	12	K.4.1.10 K.4.1.9 K.4.2.1 K.4.2.10 K.4.2.11 K.4.2.12 K.4.2.13 K.4.2.3 K.4.2.4 K.4.2.6 K.4.2.7 K.4.2.9	Feb 17, 2022 06:34:45
gke-cluster-1-default-pool-d051acb1-r9l9	Container-Optimized OS from Google	5.4.144+	2	4128243712	17	Protect	12	K.4.1.10 K.4.1.9 K.4.2.1 K.4.2.10 K.4.2.11 K.4.2.12 K.4.2.13 K.4.2.3 K.4.2.4 K.4.2.6 K.4.2.7 K.4.2.9	Feb 17, 2022 06:35:00
gke-cluster-1-default-pool-d051acb1-tztv	Container-Optimized OS from Google	5.4.144+	2	4128243712	19	Protect	12	K.4.1.10 K.4.1.9 K.4.2.1 K.4.2.10 K.4.2.11 K.4.2.12 K.4.2.13 K.4.2.3 K.4.2.4 K.4.2.6 K.4.2.7 K.4.2.9	Feb 17, 2022 06:35:11

Platforms

Name	Version	Base OS	Compliance Count	Compliance List
Kubernetes	1.21.6-gke.1500		0	

Images (Compliant Images (No Compliance Violations): 11% (1 Image(s)))

Name	Compliance Count	Compliance List
nvbeta/dns_client2:latest	5	I.4.1 I.4.10 I.4.6 I.4.8 I.4.9
nvbeta/exploit_1_21:latest	4	I.4.1 I.4.10 I.4.6 I.4.8
nvbeta/nginx:latest	4	I.4.1 I.4.10 I.4.6 I.4.8
nvbeta/swarm_nginx:latest	4	I.4.1 I.4.10 I.4.6 I.4.8
nvbeta/node:latest	4	I.4.10 I.4.6 I.4.8 I.4.9
nvbeta/api_server:latest	3	I.4.1 I.4.6 I.4.8
nvbeta/iodine:latest	3	I.4.1 I.4.6 I.4.8
nvbeta/hello-world:latest	2	I.4.1 I.4.6
k8s.gcr.io/pause@sha256:927d98197ec1141a368550822d18fa1c60bdae27b78b0c004f705f548c07814f	0	

Appendix (Full compliance list) (Show full list of compliance)

Category	Name	Description	Level	Scored	Profile	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	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	N/A
image	I.4.1	Ensure a user for the container has been created	WARN	true	Level 1	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	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	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	N/A
image	I.4.9	Ensure that COPY is used instead of ADD in Dockerfiles	WARN	false	Level 1	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	Run the following command (using the config file location identied in the Audit step) chown root:root /etc/kubernetes/kubelet.conf
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	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	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	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	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	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

Category	Name	Description	Level	Scored	Profile	remediation
						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
kubernetes	K.4.2.13	Ensure that the Kubelet only makes use of Strong Cryptographic Ciphers	WARN	false	Level 1	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	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	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
kubernetes	K.4.2.6	Ensure that the --protect-kernel-defaults argument is set to true	WARN	true	Level 1	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	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	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-

Category	Name	Description	Level	Scored	Profile	remediation
						reload systemctl restart kubelet.service