Qualys Kubernetes Posture Management

Policy Document

Qualys, Inc.
919 E Hillsdale Blvd
4th Floor
Foster City, CA 94404
1 (650) 801 6100

Table of Contents

CIS Azure Kubernetes Service (AKS) Benchmark v1.2.0

Control ID - 45001: Prevent containers from allowing command execution

Control ID - 45003: Roles with delete capabilities

Control ID - 45005: Non-root containers

Control ID - 45006: Access Kubernetes dashboard

Control ID - 45007: List Kubernetes secrets

Control ID - 45008: Allow privilege escalation

Control ID - 45009: Immutable container filesystem

Control ID - 45010: Configured readiness probe

Control ID - 45011: Mount service principal

Control ID - 45014: Ingress and Egress blocked

Control ID - 45015: Delete Kubernetes events

Control ID - 45016: Automatic mapping of service account

Control ID - 45017: Administrative Roles

Control ID - 45018: Validate admission controller (validating)

Control ID - 45019: Host PID/IPC privileges

Control ID - 45021: HostNetwork access

Control ID - 45022: SSH server running inside container

Control ID - 45023: Container hostPort

Control ID - 45024: Writable hostPath mount

Control ID - 45026: HostPath mount

Control ID - 45027: Network mapping

Control ID - 45029: Cluster internal networking

Control ID - 45030: Linux hardening

Control ID - 45031: Configured liveness probe

Control ID - 45032: Privileged container

Control ID - 45035: Pods in default namespace

Control ID - 45036: Sudo in container entrypoint

Control ID - 45037: Portforwarding privileges

Control ID - 45038: No impersonation

Control ID - 45042: Disable anonymous access to Kubelet service

Control ID - 45043: Enforce Kubelet client TLS authentication

Control ID - 45044: Naked pods

Control ID - 45045: Container runtime socket mounted

Control ID - 45046: Image pull policy on latest tag

Control ID - 45054: Anonymous user has RoleBinding

Control ID - 45055: system:authenticated user has elevated roles

Control ID - 45056: Ensure CPU limits are set

Control ID - 45057: Ensure memory limits are set

Control ID - 45060: Check if signature exists

Control ID - 45061: Missing network policy

Control ID - 45062: External facing

Control ID - 45063: Deprecated Kubernetes image registry

Control ID - 45064: Ensure CPU requests are set

Control ID - 45065: Ensure memory requests are set

Control ID - 45066: CoreDNS poisoning

Control ID - 45067: Workload with secret access

Control ID - 45068: Workload with PVC access

Control ID - 45069: Workload with ConfigMap access

Control ID - 45070: Workload with credential access

Control ID - 45071: ServiceAccount token mounted

Control ID - 45072: PersistentVolume without encryption

Control ID - 45073: Workload with cluster takeover roles

Control ID - 45074: Workload with administrative roles

Control ID - 45075: Outdated Kubernetes version

Control ID - 45076: Exposure to internet via Gateway API

Control ID - 45077: Verify Authenticated Service

Control ID - 45078: Ingress uses TLS

Control ID - 45239: Ensure that the kube-proxy metrics service is bound to localhost

Control ID – 45081: Ensure that the –kubeconfig kubelet conf file ownership is set to root:root

Control ID - 45083: Ensure that the --anonymous-auth argument is set to false

Control ID - 45084: Ensure that the --authorization-mode argument is not set to AlwaysAllow

Control ID - 45085: Ensure that the --client-ca-file argument is set as appropriate

Control ID - 45086: Verify that the --read-only-port argument is set to 0

Control ID - 45087: Ensure that the --streaming-connection-idle-timeout argument is not set to 0

Control ID - 45089: Ensure that the --make-iptables-util-chains argument is set to true

Control ID - 45091: Ensure that the eventRecordQPS argument is set to a level which ensures appropriate event capture

Control ID - 45092: Ensure that the --rotate-certificates argument is not set to false

Control ID - 45093: Verify that the RotateKubeletServerCertificate argument is set to true

Control ID - 45094: Ensure that the cluster-admin role is only used where required

Control ID - 45095: Minimize access to secrets

Control ID - 45096: Minimize wildcard use in Roles and ClusterRoles

Control ID - 45097: Minimize access to create pods

Control ID - 45098: Ensure that default service accounts are not actively used

Control ID - 45099: Ensure that Service Account Tokens are only mounted where necessary

Control ID - 45102: Ensure that all Namespaces have Network Policies defined

Control ID - 45103: Prefer using secrets as files over secrets as environment variables

Control ID - 45104: Consider external secret storage

Control ID - 45105: Create administrative boundaries between resources using namespaces

Control ID - 45106: Apply Security Context to Your Pods and Containers

Control ID - 45107: The default namespace should not be used

Control ID - 45226: Minimize the admission of privileged containers

Control ID - 45227: Minimize the admission of containers wishing to share the host process ID namespace

Control ID - 45228: Minimize the admission of containers wishing to share the host IPC namespace

Control ID - 45229: Minimize the admission of containers wishing to share the host network namespace

Control ID - 45230: Minimize the admission of containers with allowPrivilegeEscalation

Control ID - 45117: Prefer using dedicated AKS Service Accounts

Control ID - 45123: Encrypt traffic to HTTPS load balancers with TLS certificates

Control ID - 45128: Minimize user access to Azure Container Registry (ACR)

Azure Kubernetes Service (AKS) Best Practices

Control ID - 45001: Prevent containers from allowing command execution

Control ID - 45003: Roles with delete capabilities

Control ID - 45005: Non-root containers

Control ID - 45006: Access Kubernetes dashboard

Control ID - 45007: List Kubernetes secrets

Control ID - 45008: Allow privilege escalation

Control ID - 45009: Immutable container filesystem

Control ID - 45010: Configured readiness probe

Control ID - 45011: Mount service principal

Control ID - 45014: Ingress and Egress blocked

Control ID - 45015: Delete Kubernetes events

Control ID - 45016: Automatic mapping of service account

Control ID - 45017: Administrative Roles

Control ID - 45018: Validate admission controller (validating)

Control ID - 45019: Host PID/IPC privileges

Control ID - 45021: HostNetwork access

Control ID - 45022: SSH server running inside container

Control ID - 45023: Container hostPort

Control ID - 45024: Writable hostPath mount

Control ID - 45026: HostPath mount

Control ID - 45027: Network mapping

Control ID - 45029: Cluster internal networking

Control ID - 45030: Linux hardening

Control ID - 45031: Configured liveness probe

Control ID - 45032: Privileged container

Control ID - 45035: Pods in default namespace

Control ID - 45036: Sudo in container entrypoint

Control ID - 45037: Portforwarding privileges

Control ID - 45038: No impersonation

Control ID - 45042: Disable anonymous access to Kubelet service

Control ID - 45043: Enforce Kubelet client TLS authentication

Control ID - 45044: Naked pods

Control ID - 45045: Container runtime socket mounted

Control ID - 45046: Image pull policy on latest tag

Control ID - 45054: Anonymous user has RoleBinding

Control ID - 45055: system:authenticated user has elevated roles

Control ID - 45056: Ensure CPU limits are set

Control ID - 45057: Ensure memory limits are set

Control ID - 45060: Check if signature exists

Control ID - 45061: Missing network policy

Control ID - 45062: External facing

Control ID - 45063: Deprecated Kubernetes image registry

Control ID - 45064: Ensure CPU requests are set

Control ID - 45065: Ensure memory requests are set

Control ID - 45066: CoreDNS poisoning

Control ID - 45067: Workload with secret access

Control ID - 45068: Workload with PVC access

Control ID - 45069: Workload with ConfigMap access

Control ID - 45070: Workload with credential access

Control ID - 45071: ServiceAccount token mounted

Control ID - 45072: PersistentVolume without encryption

Control ID - 45073: Workload with cluster takeover roles

Control ID - 45074: Workload with administrative roles

Control ID - 45075: Outdated Kubernetes version

Control ID - 45076: Exposure to internet via Gateway API

Control ID - 45077: Verify Authenticated Service

Control ID - 45078: Ingress uses TLS

Control ID - 45239: Ensure that the kube-proxy metrics service is bound to localhost

AWS Elastic Kubernetes Service (EKS) Best Practices

Control ID - 45001: Prevent containers from allowing command execution

Control ID - 45003: Roles with delete capabilities

Control ID - 45005: Non-root containers

Control ID - 45006: Access Kubernetes dashboard

Control ID - 45007: List Kubernetes secrets

Control ID - 45008: Allow privilege escalation

Control ID - 45009: Immutable container filesystem

Control ID - 45010: Configured readiness probe

Control ID - 45011: Mount service principal

Control ID - 45014: Ingress and Egress blocked

Control ID - 45015: Delete Kubernetes events

Control ID - 45016: Automatic mapping of service account

Control ID - 45017: Administrative Roles

Control ID - 45018: Validate admission controller (validating)

Control ID - 45019: Host PID/IPC privileges

Control ID - 45021: HostNetwork access

Control ID - 45022: SSH server running inside container

Control ID - 45023: Container hostPort

Control ID - 45024: Writable hostPath mount

Control ID - 45026: HostPath mount

Control ID - 45027: Network mapping

Control ID - 45029: Cluster internal networking

Control ID - 45030: Linux hardening

Control ID - 45031: Configured liveness probe

Control ID - 45032: Privileged container

Control ID - 45035: Pods in default namespace

Control ID - 45036: Sudo in container entrypoint

Control ID - 45037: Portforwarding privileges

Control ID - 45038: No impersonation

Control ID - 45042: Disable anonymous access to Kubelet service

Control ID - 45043: Enforce Kubelet client TLS authentication

Control ID - 45044: Naked pods

Control ID - 45045: Container runtime socket mounted

Control ID - 45046: Image pull policy on latest tag

Control ID - 45054: Anonymous user has RoleBinding

Control ID - 45055: system:authenticated user has elevated roles

Control ID - 45056: Ensure CPU limits are set

Control ID - 45057: Ensure memory limits are set

Control ID - 45060: Check if signature exists

Control ID - 45061: Missing network policy

Control ID - 45062: External facing

Control ID - 45063: Deprecated Kubernetes image registry

Control ID - 45064: Ensure CPU requests are set

Control ID - 45065: Ensure memory requests are set

Control ID - 45066: CoreDNS poisoning

Control ID - 45067: Workload with secret access

Control ID - 45068: Workload with PVC access

Control ID - 45069: Workload with ConfigMap access

Control ID - 45070: Workload with credential access

Control ID - 45071: ServiceAccount token mounted

Control ID - 45072: PersistentVolume without encyption

Control ID - 45073: Workload with cluster takeover roles

Control ID - 45074: Workload with administrative roles

Control ID - 45075: Outdated Kubernetes version

Control ID - 45076: Exposure to internet via Gateway API

Control ID - 45077: Verify Authenticated Service

Control ID - 45078: Ingress uses TLS

Control ID - 45239: Ensure that the kube-proxy metrics service is bound to localhost

Control ID - 45106: Apply Security Context to Your Pods and Containers

CIS Amazon Elastic Kubernetes Service (EKS) Benchmark v1.2.0

Control ID - 45081: Ensure that the --kubeconfig kubelet.conf file ownership is set to root:root

Control ID - 45082: If the kubelet config.yaml configuration file is being used validate file ownership is set to root:root

Control ID - 45083: Ensure that the --anonymous-auth argument is set to false

Control ID - 45084: Ensure that the --authorization-mode argument is not set to AlwaysAllow

Control ID - 45085: Ensure that the --client-ca-file argument is set as appropriate

Control ID - 45086: Verify that the --read-only-port argument is set to 0

Control ID - 45087: Ensure that the --streaming-connection-idle-timeout argument is not set to 0

Control ID - 45088: Ensure that the --protect-kernel-defaults argument is set to true

Control ID - 45089: Ensure that the --make-iptables-util-chains argument is set to true

Control ID - 45090: Ensure that the --hostname-override argument is not set

Control ID - 45091: Ensure that the eventRecordQPS argument is set to a level which ensures appropriate event capture

Control ID - 45131: Ensure that the --tls-cert-file and --tls-private-key-file arguments are set as appropriate

Control ID - 45093: Verify that the RotateKubeletServerCertificate argument is set to true

Control ID - 45094: Ensure that the cluster-admin role is only used where required

Control ID - 45095: Minimize access to secrets

Control ID - 45096: Minimize wildcard use in Roles and ClusterRoles

Control ID - 45097: Minimize access to create pods

Control ID - 45098: Ensure that default service accounts are not actively used

Control ID - 45099: Ensure that Service Account Tokens are only mounted where necessary

Control ID - 45132: Limit use of the Bind, Impersonate and Escalate permissions in the Kubernetes cluster

Control ID - 45101: Ensure that the CNI in use supports Network Policies

Control ID - 45102: Ensure that all Namespaces have Network Policies defined

Control ID - 45103: Prefer using secrets as files over secrets as environment variables

Control ID - 45105: Create administrative boundaries between resources using namespaces

Control ID - 45106: Apply Security Context to Your Pods and Containers

Control ID - 45107: The default namespace should not be used

Control ID - 45108: Minimize the admission of privileged containers

Control ID - 45109: Minimize the admission of containers wishing to share the host process ID namespace

Control ID - 45110: Minimize the admission of containers wishing to share the host IPC namespace

Control ID - 45111: Minimize the admission of containers wishing to share the host network namespace

Control ID - 45112: Minimize the admission of containers with allowPrivilegeEscalation

Control ID - 45113: Minimize the admission of root containers

Control ID - 45114: Minimize the admission of containers with added capabilities

Control ID - 45133: Minimize the admission of containers with capabilities assigned

Control ID - 45136: Prefer using dedicated EKS Service Accounts

Control ID - 45137: Prefer using a container-optimized OS when possible

Control ID - 45140: Ensure Network Policy is Enabled and set as appropriate

Control ID - 45141: Encrypt traffic to HTTPS load balancers with TLS certificates

Control ID - 45142: Manage Kubernetes RBAC users with AWS IAM Authenticator for Kubernetes or Upgrade to AWS CLI v1.16.156

Control ID - 45143: Consider Fargate for running untrusted workloads

Control ID - 45144: Consider external secret storage

Control ID - 45115: Ensure that the kubelet configuration file has permissions set to 644 or more restrictive

Control ID - 45116: Ensure that the kubeconfig file permissions are set to 644 or more restrictive

Control ID - 45081: Ensure that the --kubeconfig kubelet.conf file ownership is set to root:root

Control ID - 45082: If the kubelet config.yaml configuration file is being used validate file ownership is set to root:root

Control ID - 45083: Ensure that the --anonymous-auth argument is set to false

Control ID - 45084: Ensure that the --authorization-mode argument is not set to AlwaysAllow

Control ID - 45085: Ensure that the --client-ca-file argument is set as appropriate

Control ID - 45086: Verify that the --read-only-port argument is set to 0

Control ID - 45087: Ensure that the --streaming-connection-idle-timeout argument is not set to 0

Control ID - 45088: Ensure that the --protect-kernel-defaults argument is set to true

Control ID - 45089: Ensure that the --make-iptables-util-chains argument is set to true

Control ID - 45090: Ensure that the --hostname-override argument is not set

Control ID - 45091: Ensure that the eventRecordQPS argument is set to a level which ensures appropriate event capture

Control ID - 45131: Ensure that the --tls-cert-file and --tls-private-key-file arguments are set as appropriate

Control ID - 45093: Verify that the RotateKubeletServerCertificate argument is set to true

Control ID - 45094: Ensure that the cluster-admin role is only used where required

Control ID - 45095: Minimize access to secrets

Control ID - 45096: Minimize wildcard use in Roles and ClusterRoles

Control ID - 45097: Minimize access to create pods

Control ID - 45098: Ensure that default service accounts are not actively used

Control ID - 45099: Ensure that Service Account Tokens are only mounted where necessary

Control ID - 45132: Limit use of the Bind, Impersonate and Escalate permissions in the Kubernetes cluster

Control ID - 45101: Ensure that the CNI in use supports Network Policies

Control ID - 45102: Ensure that all Namespaces have Network Policies defined

Control ID - 45103: Prefer using secrets as files over secrets as environment variables

Control ID - 45105: Create administrative boundaries between resources using namespaces

Control ID - 45106: Apply Security Context to Your Pods and Containers

Control ID - 45107: The default namespace should not be used

Control ID - 45108: Minimize the admission of privileged containers

Control ID - 45109: Minimize the admission of containers wishing to share the host process ID namespace

Control ID - 45110: Minimize the admission of containers wishing to share the host IPC namespace

Control ID - 45111: Minimize the admission of containers wishing to share the host network namespace

Control ID - 45112: Minimize the admission of containers with allowPrivilegeEscalation

Control ID - 45113: Minimize the admission of root containers

Control ID - 45114: Minimize the admission of containers with added capabilities

Control ID - 45133: Minimize the admission of containers with capabilities assigned

Control ID - 45136: Prefer using dedicated EKS Service Accounts

Control ID - 45137: Prefer using a container-optimized OS when possible

Control ID - 45140: Ensure Network Policy is Enabled and set as appropriate

Control ID - 45141: Encrypt traffic to HTTPS load balancers with TLS certificates

Control ID - 45142: Manage Kubernetes RBAC users with AWS IAM Authenticator for Kubernetes or Upgrade to AWS CLI v1.16.156

Control ID - 45143: Consider Fargate for running untrusted workloads

Control ID - 45144: Consider external secret storage

Control ID - 45115: Ensure that the kubelet configuration file has permissions set to 644 or more restrictive

Control ID - 45116: Ensure that the kubeconfig file permissions are set to 644 or more restrictive

Control ID - 45081: Ensure that the --kubeconfig kubelet.conf file ownership is set to root:root

Control ID - 45082: If the kubelet config.yaml configuration file is being used validate file ownership is set to root:root

Control ID - 45083: Ensure that the --anonymous-auth argument is set to false

Control ID - 45084: Ensure that the --authorization-mode argument is not set to AlwaysAllow

Control ID - 45085: Ensure that the --client-ca-file argument is set as appropriate

Control ID - 45086: Verify that the --read-only-port argument is set to 0

Control ID - 45087: Ensure that the --streaming-connection-idle-timeout argument is not set to 0

Control ID - 45089: Ensure that the --make-iptables-util-chains argument is set to true

Control ID - 45115: Ensure that the kubelet configuration file has permissions set to 644 or more restrictive

Control ID - 45116: Ensure that the kubeconfig file permissions are set to 644 or more restrictive

Control ID - 45092: Ensure that the --rotate-certificates argument is not set to false

Control ID - 45093: Verify that the RotateKubeletServerCertificate argument is set to true

Control ID - 45094: Ensure that the cluster-admin role is only used where required

Control ID - 45095: Minimize access to secrets

Control ID - 45096: Minimize wildcard use in Roles and ClusterRoles

Control ID - 45097: Minimize access to create pods

Control ID - 45098: Ensure that default service accounts are not actively used

Control ID - 45099: Ensure that Service Account Tokens are only mounted where necessary

Control ID - 45132: Limit use of the Bind, Impersonate and Escalate permissions in the Kubernetes cluster

Control ID - 45226: Minimize the admission of privileged containers

Control ID - 45227: Minimize the admission of containers wishing to share the host process ID namespace

Control ID - 45228: Minimize the admission of containers wishing to share the host IPC namespace

Control ID - 45229: Minimize the admission of containers wishing to share the host network namespace

Control ID - 45230: Minimize the admission of containers with allowPrivilegeEscalation

Control ID - 45101: Ensure that the CNI in use supports Network Policies

Control ID - 45102: Ensure that all Namespaces have Network Policies defined

Control ID - 45103: Prefer using secrets as files over secrets as environment variables

Control ID - 45144: Consider external secret storage

Control ID - 45105: Create administrative boundaries between resources using namespaces

Control ID - 45107: The default namespace should not be used

Control ID - 45136: Prefer using dedicated EKS Service Accounts

Control ID - 45140: Ensure Network Policy is Enabled and set as appropriate

Control ID - 45141: Encrypt traffic to HTTPS load balancers with TLS certificates

Control ID - 45142: Manage Kubernetes RBAC users with AWS IAM Authenticator for Kubernetes or Upgrade to AWS CLI v1.16.156

Control ID - 45091: Ensure that the eventRecordQPS argument is set to a level which ensures appropriate event capture

Google Kubernetes Engine (GKE) Best Practices

Control ID - 45001: Prevent containers from allowing command execution

Control ID - 45003: Roles with delete capabilities

Control ID - 45005: Non-root containers

Control ID - 45006: Access Kubernetes dashboard

Control ID - 45007: List Kubernetes secrets

Control ID - 45008: Allow privilege escalation

Control ID - 45009: Immutable container filesystem

Control ID - 45010: Configured readiness probe

Control ID - 45011: Mount service principal

Control ID - 45014: Ingress and Egress blocked

Control ID - 45015: Delete Kubernetes events

Control ID - 45016: Automatic mapping of service account

Control ID - 45017: Administrative Roles

Control ID - 45018: Validate admission controller (validating)

Control ID - 45019: Host PID/IPC privileges

Control ID - 45021: HostNetwork access

Control ID - 45022: SSH server running inside container

Control ID - 45023: Container hostPort

Control ID - 45024: Writable hostPath mount

Control ID - 45026: HostPath mount

Control ID - 45027: Network mapping

Control ID - 45029: Cluster internal networking

Control ID - 45030: Linux hardening

Control ID - 45031: Configured liveness probe

Control ID - 45032: Privileged container

Control ID - 45035: Pods in default namespace

Control ID - 45036: Sudo in container entrypoint

Control ID - 45037: Portforwarding privileges

Control ID - 45038: No impersonation

Control ID - 45042: Disable anonymous access to Kubelet service

Control ID - 45043: Enforce Kubelet client TLS authentication

Control ID - 45044: Naked pods

Control ID - 45045: Container runtime socket mounted

Control ID - 45046: Image pull policy on latest tag

Control ID - 45054: Anonymous user has RoleBinding

Control ID - 45055: system:authenticated user has elevated roles

Control ID - 45056: Ensure CPU limits are set

Control ID - 45057: Ensure memory limits are set

Control ID - 45060: Check if signature exists

Control ID - 45097: Minimize access to create pods

Control ID - 45061: Missing network policy

Control ID - 45062: External facing

Control ID - 45063: Deprecated Kubernetes image registry

Control ID - 45064: Ensure CPU requests are set

Control ID - 45065: Ensure memory requests are set

Control ID - 45066: CoreDNS poisoning

Control ID - 45067: Workload with secret access

Control ID - 45068: Workload with PVC access

Control ID - 45069: Workload with ConfigMap access

Control ID - 45070: Workload with credential access

Control ID - 45071: ServiceAccount token mounted

Control ID - 45072: PersistentVolume without encryption

Control ID - 45073: Workload with cluster takeover roles

Control ID - 45074: Workload with administrative roles

Control ID - 45075: Outdated Kubernetes version

Control ID - 45076: Exposure to internet via Gateway API

Control ID - 45077: Verify Authenticated Service

Control ID - 45078: Ingress uses TLS

Control ID - 45103: Prefer using secrets as files over secrets as environment variables

Control ID - 45094: Ensure that the cluster-admin role is only used where required

Control ID - 45095: Minimize access to secrets

Control ID - 45096: Minimize wildcard use in Roles and ClusterRoles

Control ID - 45098: Ensure that default service accounts are not actively used

Control ID - 45099: Ensure that Service Account Tokens are only mounted where necessary

Control ID - 45132: Limit use of the Bind, Impersonate and Escalate permissions in the Kubernetes cluster

Control ID - 45102: Ensure that all Namespaces have Network Policies defined

Control ID - 45144: Consider external secret storage

Control ID - 45105: Create administrative boundaries between resources using namespaces

Control ID - 45106: Apply Security Context to Your Pods and Containers

Control ID - 45107: The default namespace should not be used

Control ID - 45094: Ensure that the cluster-admin role is only used where required

Control ID - 45095: Minimize access to secrets

Control ID - 45096: Minimize wildcard use in Roles and ClusterRoles

Control ID - 45098: Ensure that default service accounts are not actively used

Control ID - 45099: Ensure that Service Account Tokens are only mounted where necessary

Control ID - 45132: Limit use of the Bind, Impersonate and Escalate permissions in the Kubernetes cluster

Control ID - 45101: Ensure that the CNI in use supports Network Policies

Control ID - 45102: Ensure that all Namespaces have Network Policies defined

Control ID - 45103: Prefer using secrets as files over secrets as environment variables

Control ID - 45104: Consider external secret storage

Control ID - 45105: Create administrative boundaries between resources using namespaces

Control ID - 45237: Ensure that the seccomp profile is set to docker/default in your pod definitions

Control ID - 45106: Apply Security Context to Your Pods and Containers

Control ID - 45107: The default namespace should not be used

Control ID - 45098: Ensure that default service accounts are not actively used

Kubernetes Best Practices

Control ID - 45001: Prevent containers from allowing command execution

Control ID - 45002: API server insecure port is enabled

Control ID - 45003: Roles with delete capabilities

Control ID - 45005: Non-root containers

Control ID - 45006: Access Kubernetes dashboard

Control ID - 45007: List Kubernetes secrets

Control ID - 45008: Allow privilege escalation

Control ID - 45009: Immutable container filesystem

Control ID - 45010: Configured readiness probe

Control ID - 45011: Mount service principal

Control ID - 45014: Ingress and Egress blocked

Control ID - 45015: Delete Kubernetes events

Control ID - 45016: Automatic mapping of service account

Control ID - 45017: Administrative Roles

Control ID - 45018: Validate admission controller (validating)

Control ID - 45019: Host PID/IPC privileges

Control ID - 45021: HostNetwork access

Control ID - 45022: SSH server running inside container

Control ID - 45023: Container hostPort

Control ID - 45024: Writable hostPath mount

Control ID - 45026: HostPath mount

Control ID - 45027: Network mapping

Control ID - 45029: Cluster internal networking

Control ID - 45030: Linux hardening

Control ID - 45031: Configured liveness probe

Control ID - 45032: Privileged container

Control ID - 45035: Pods in default namespace

Control ID - 45036: Sudo in container entrypoint

Control ID - 45037: Portforwarding privileges

Control ID - 45038: No impersonation

Control ID - 45039: Secret/etcd encryption enabled

Control ID - 45040: Audit logs enabled

Control ID - 45041: PSP enabled

Control ID - 45042: Disable anonymous access to Kubelet service

Control ID - 45043: Enforce Kubelet client TLS authentication

Control ID - 45044: Naked pods

Control ID - 45045: Container runtime socket mounted

Control ID - 45046: Image pull policy on latest tag

Control ID - 45080: RBAC enabled

Control ID - 45054: Anonymous user has RoleBinding

Control ID - 45055: system:authenticated user has elevated roles

Control ID - 45056: Ensure CPU limits are set

Control ID - 45057: Ensure memory limits are set

Control ID - 45060: Check if signature exists

Control ID - 45061: Missing network policy

Control ID - 45062: External facing

Control ID - 45063: Deprecated Kubernetes image registry

Control ID - 45064: Ensure CPU requests are set

Control ID - 45065: Ensure memory requests are set

Control ID - 45066: CoreDNS poisoning

Control ID - 45067: Workload with secret access

Control ID - 45068: Workload with PVC access

Control ID - 45069: Workload with ConfigMap access

Control ID - 45070: Workload with credential access

Control ID - 45071: ServiceAccount token mounted

Control ID - 45072: PersistentVolume without encyption

Control ID - 45073: Workload with cluster takeover roles

Control ID - 45074: Workload with administrative roles

Control ID - 45075: Outdated Kubernetes version

Control ID - 45076: Exposure to internet via Gateway API

Control ID - 45077: Verify Authenticated Service

Control ID - 45078: Ingress uses TLS

Control ID - 45239: Ensure that the kube-proxy metrics service is bound to localhost

Control ID - 45146: Ensure that the API server pod specification file permissions are set to 600 or more restrictive

Control ID - 45147: Ensure that the API server pod specification file ownership is set to root:root

Control ID - 45148: Ensure that the controller manager pod specification file permissions are set to 600 or more restrictive

Control ID - 45149: Ensure that the controller manager pod specification file ownership is set to root:root

Control ID - 45150: Ensure that the scheduler pod specification file permissions are set to 600 or more restrictive

Control ID - 45151: Ensure that the scheduler pod specification file ownership is set to root:root

Control ID - 45152: Ensure that the etcd pod specification file permissions are set to 600 or more restrictive

Control ID - 45153: Ensure that the etcd pod specification file ownership is set to root:root

Control ID - 45154: Ensure that the Container Network Interface file permissions are set to 600 or more restrictive

Control ID - 45155: Ensure that the Container Network Interface file ownership is set to root:root

Control ID - 45156: Ensure that the etcd data directory permissions are set to 700 or more restrictive

Control ID - 45157: Ensure that the etcd data directory ownership is set to etcd:etcd

Control ID - 45158: Ensure that the admin.conf file permissions are set to 600

Control ID - 45159: Ensure that the admin.conf file ownership is set to root:root

Control ID - 45160: Ensure that the scheduler.conf file permissions are set to 600 or more restrictive

Control ID - 45161: Ensure that the scheduler.conf file ownership is set to root:root

Control ID - 45162: Ensure that the controller-manager.conf file permissions are set to 600 or more restrictive

Control ID - 45163: Ensure that the controller-manager.conf file ownership is set to root:root

Control ID - 45164: Ensure that the Kubernetes PKI directory and file ownership is set to root:root

Control ID - 45165: Ensure that the Kubernetes PKI certificate file permissions are set to 600 or more restrictive

Control ID - 45166: Ensure that the Kubernetes PKI key file permissions are set to 600

Control ID - 45167: Ensure that the API Server --anonymous-auth argument is set to false

Control ID - 45168: Ensure that the API Server --token-auth-file parameter is not set

Control ID - 45169: Ensure that the API Server --DenyServiceExternalIPs is not set

Control ID - 45170: Ensure that the API Server --kubelet-client-certificate and --kubelet-client-key arguments are set as appropriate

Control ID - 45171: Ensure that the API Server --kubelet-certificate-authority argument is set as appropriate

Control ID - 45172: Ensure that the API Server --authorization-mode argument is not set to AlwaysAllow

Control ID - 45173: Ensure that the API Server --authorization-mode argument includes Node

Control ID - 45174: Ensure that the API Server --authorization-mode argument includes RBAC

Control ID - 45175: Ensure that the admission control plugin EventRateLimit is set

Control ID - 45176: Ensure that the admission control plugin AlwaysAdmit is not set

Control ID - 45177: Ensure that the admission control plugin AlwaysPullImages is set

Control ID - 45178: Ensure that the admission control plugin SecurityContextDeny is set if PodSecurityPolicy is not used

Control ID - 45179: Ensure that the admission control plugin ServiceAccount is set

Control ID - 45180: Ensure that the admission control plugin NamespaceLifecycle is set

Control ID - 45181: Ensure that the admission control plugin NodeRestriction is set

Control ID - 45182: Ensure that the API Server --secure-port argument is not set to 0

Control ID - 45183: Ensure that the API Server --profiling argument is set to false

Control ID - 45184: Ensure that the API Server --audit-log-path argument is set

Control ID - 45185: Ensure that the API Server --audit-log-maxage argument is set to 30 or as appropriate

Control ID - 45186: Ensure that the API Server --audit-log-maxbackup argument is set to 10 or as appropriate

Control ID - 45187: Ensure that the API Server --audit-log-maxsize argument is set to 100 or as appropriate

Control ID - 45188: Ensure that the API Server --request-timeout argument is set as appropriate

Control ID - 45189: Ensure that the API Server --service-account-lookup argument is set to true

Control ID - 45190: Ensure that the API Server --service-account-key-file argument is set as appropriate

Control ID - 45191: Ensure that the API Server --etcd-certfile and --etcd-keyfile arguments are set as appropriate

Control ID - 45192: Ensure that the API Server --tls-cert-file and --tls-private-key-file arguments are set as appropriate

Control ID - 45193: Ensure that the API Server --client-ca-file argument is set as appropriate

Control ID - 45194: Ensure that the API Server --etcd-cafile argument is set as appropriate

Control ID - 45195: Ensure that the API Server --encryption-provider-config argument is set as appropriate

Control ID - 45196: Ensure that encryption providers are appropriately configured

Control ID - 45197: Ensure that the API Server only makes use of Strong Cryptographic Ciphers

Control ID - 45198: Ensure that the Controller Manager --terminated-pod-gc-threshold argument is set as appropriate

Control ID - 45199: Ensure that the Controller Manager --profiling argument is set to false

Control ID - 45200: Ensure that the Controller Manager --use-service-account-credentials argument is set to true

Control ID - 45201: Ensure that the Controller Manager --service-account-private-key-file argument is set as appropriate

Control ID - 45202: Ensure that the Controller Manager --root-ca-file argument is set as appropriate

Control ID - 45203: Ensure that the Controller Manager RotateKubeletServerCertificate argument is set to true

Control ID - 45204: Ensure that the Controller Manager --bind-address argument is set to 127.0.0.1

Control ID - 45205: Ensure that the Scheduler --profiling argument is set to false

Control ID - 45206: Ensure that the Scheduler --bind-address argument is set to 127.0.0.1

Control ID - 45207: Ensure that the --cert-file and --key-file arguments are set as appropriate

Control ID - 45208: Ensure that the --client-cert-auth argument is set to true

Control ID - 45209: Ensure that the --auto-TLS argument is not set to true

Control ID - 45210: Ensure that the --peer-cert-file and --peer-key-file arguments are set as appropriate

Control ID - 45211: Ensure that the --peer-client-cert-auth argument is set to true

Control ID - 45212: Ensure that the --peer-auto-tls argument is not set to true

Control ID - 45213: Ensure that a unique Certificate Authority is used for etcd

Control ID - 45214: Ensure that a minimal audit policy is created

Control ID - 45215: Ensure that the audit policy covers key security concerns

Control ID - 45216: Ensure that the kubelet service file permissions are set to 600 or more restrictive

Control ID - 45217: Ensure that the kubelet service file ownership is set to root:root

Control ID - 45218: If proxy kubeconfig file exists ensure permissions are set to 600 or more restrictive

Control ID - 45219: If proxy kubeconfig file exists ensure ownership is set to root:root

Control ID - 45220: Ensure that the --kubeconfig kubelet.conf file permissions are set to 600 or more restrictive

Control ID - 45081: Ensure that the --kubeconfig kubelet.conf file ownership is set to root:root

Control ID - 45221: Ensure that the certificate authorities file permissions are set to 600 or more restrictive

Control ID - 45222: Ensure that the client certificate authorities file ownership is set to root:root

Control ID - 45223: If the kubelet config.yaml configuration file is being used validate permissions set to 600 or more restrictive

Control ID - 45082: If the kubelet config.yaml configuration file is being used validate file ownership is set to root:root

Control ID - 45083: Ensure that the --anonymous-auth argument is set to false

Control ID - 45084: Ensure that the --authorization-mode argument is not set to AlwaysAllow

Control ID - 45085: Ensure that the --client-ca-file argument is set as appropriate

Control ID - 45086: Verify that the --read-only-port argument is set to 0

Control ID - 45087: Ensure that the --streaming-connection-idle-timeout argument is not set to 0

Control ID - 45088: Ensure that the --protect-kernel-defaults argument is set to true

Control ID - 45089: Ensure that the --make-iptables-util-chains argument is set to true

Control ID - 45090: Ensure that the --hostname-override argument is not set

Control ID - 45091: Ensure that the eventRecordQPS argument is set to a level which ensures appropriate event capture

Control ID - 45131: Ensure that the --tls-cert-file and --tls-private-key-file arguments are set as appropriate

Control ID - 45092: Ensure that the --rotate-certificates argument is not set to false

Control ID - 45093: Verify that the RotateKubeletServerCertificate argument is set to true

Control ID - 45224: Ensure that the Kubelet only makes use of Strong Cryptographic Ciphers

Control ID - 45094: Ensure that the cluster-admin role is only used where required

Control ID - 45095: Minimize access to secrets

Control ID - 45096: Minimize wildcard use in Roles and ClusterRoles

Control ID - 45097: Minimize access to create pods

Control ID - 45098: Ensure that default service accounts are not actively used

Control ID - 45099: Ensure that Service Account Tokens are only mounted where necessary

Control ID - 45132: Limit use of the Bind, Impersonate and Escalate permissions in the Kubernetes cluster

Control ID - 45225: Ensure that the cluster has at least one active policy control mechanism in place

Control ID - 45226: Minimize the admission of privileged containers

Control ID - 45227: Minimize the admission of containers wishing to share the host process ID namespace

Control ID - 45228: Minimize the admission of containers wishing to share the host IPC namespace

Control ID - 45229: Minimize the admission of containers wishing to share the host network namespace

Control ID - 45230: Minimize the admission of containers with allowPrivilegeEscalation

Control ID - 45231: Minimize the admission of root containers

Control ID - 45232: Minimize the admission of containers with the NET_RAW capability

Control ID - 45233: Minimize the admission of containers with added capabilities

Control ID - 45100: Minimize the admission of containers with capabilities assigned

Control ID - 45234: Minimize the admission of Windows HostProcess Containers

Control ID - 45235: Minimize the admission of HostPath volumes

Control ID - 45236: Minimize the admission of containers which use HostPorts

Control ID - 45101: Ensure that the CNI in use supports Network Policies

Control ID - 45102: Ensure that all Namespaces have Network Policies defined

Control ID - 45103: Prefer using secrets as files over secrets as environment variables

Control ID - 45104: Consider external secret storage

Control ID - 45105: Create administrative boundaries between resources using namespaces

Control ID - 45237: Ensure that the seccomp profile is set to docker/default in your pod definitions

Control ID - 45106: Apply Security Context to Your Pods and Containers

Control ID - 45107: The default namespace should not be used

Control ID - 45146: Ensure that the API server pod specification file permissions are set to 600 or more restrictive

Control ID - 45147: Ensure that the API server pod specification file ownership is set to root:root

Control ID - 45148: Ensure that the controller manager pod specification file permissions are set to 600 or more restrictive

Control ID - 45149: Ensure that the controller manager pod specification file ownership is set to root:root

Control ID - 45150: Ensure that the scheduler pod specification file permissions are set to 600 or more restrictive

Control ID - 45151: Ensure that the scheduler pod specification file ownership is set to root:root

Control ID - 45152: Ensure that the etcd pod specification file permissions are set to 600 or more restrictive

Control ID - 45153: Ensure that the etcd pod specification file ownership is set to root:root

Control ID - 45154: Ensure that the Container Network Interface file permissions are set to 600 or more restrictive

Control ID - 45155: Ensure that the Container Network Interface file ownership is set to root:root

Control ID - 45156: Ensure that the etcd data directory permissions are set to 700 or more restrictive

Control ID - 45157: Ensure that the etcd data directory ownership is set to etcd:etcd

Control ID - 45158: Ensure that the admin.conf file permissions are set to 600

Control ID - 45159: Ensure that the admin.conf file ownership is set to root:root

Control ID - 45160: Ensure that the scheduler.conf file permissions are set to 600 or more restrictive

Control ID - 45161: Ensure that the scheduler.conf file ownership is set to root:root

Control ID - 45162: Ensure that the controller-manager.conf file permissions are set to 600 or more restrictive

Control ID - 45163: Ensure that the controller-manager.conf file ownership is set to root:root

Control ID - 45164: Ensure that the Kubernetes PKI directory and file ownership is set to root:root

Control ID - 45165: Ensure that the Kubernetes PKI certificate file permissions are set to 600 or more restrictive

Control ID - 45166: Ensure that the Kubernetes PKI key file permissions are set to 600

Control ID - 45167: Ensure that the API Server --anonymous-auth argument is set to false

Control ID - 45168: Ensure that the API Server --token-auth-file parameter is not set

Control ID - 45169: Ensure that the API Server --DenyServiceExternalIPs is not set

Control ID - 45170: Ensure that the API Server --kubelet-client-certificate and --kubelet-client-key arguments are set as appropriate

Control ID - 45171: Ensure that the API Server --kubelet-certificate-authority argument is set as appropriate

Control ID - 45172: Ensure that the API Server --authorization-mode argument is not set to AlwaysAllow

Control ID - 45173: Ensure that the API Server --authorization-mode argument includes Node

Control ID - 45174: Ensure that the API Server --authorization-mode argument includes RBAC

Control ID - 45175: Ensure that the admission control plugin EventRateLimit is set

Control ID - 45176: Ensure that the admission control plugin AlwaysAdmit is not set

Control ID - 45177: Ensure that the admission control plugin AlwaysPullImages is set

Control ID - 45179: Ensure that the admission control plugin ServiceAccount is set

Control ID - 45180: Ensure that the admission control plugin NamespaceLifecycle is set

Control ID - 45181: Ensure that the admission control plugin NodeRestriction is set

Control ID - 45183: Ensure that the API Server --profiling argument is set to false

Control ID - 45184: Ensure that the API Server --audit-log-path argument is set

Control ID - 45185: Ensure that the API Server --audit-log-maxage argument is set to 30 or as appropriate

Control ID - 45186: Ensure that the API Server --audit-log-maxbackup argument is set to 10 or as appropriate

Control ID - 45187: Ensure that the API Server --audit-log-maxsize argument is set to 100 or as appropriate

Control ID - 45188: Ensure that the API Server --request-timeout argument is set as appropriate

Control ID - 45189: Ensure that the API Server --service-account-lookup argument is set to true

Control ID - 45190: Ensure that the API Server --service-account-key-file argument is set as appropriate

Control ID - 45191: Ensure that the API Server --etcd-certfile and --etcd-keyfile arguments are set as appropriate

Control ID - 45192: Ensure that the API Server --tls-cert-file and --tls-private-key-file arguments are set as appropriate

Control ID - 45193: Ensure that the API Server --client-ca-file argument is set as appropriate

Control ID - 45194: Ensure that the API Server --etcd-cafile argument is set as appropriate

Control ID - 45195: Ensure that the API Server --encryption-provider-config argument is set as appropriate

Control ID - 45196: Ensure that encryption providers are appropriately configured

Control ID - 45197: Ensure that the API Server only makes use of Strong Cryptographic Ciphers

Control ID - 45198: Ensure that the Controller Manager --terminated-pod-gc-threshold argument is set as appropriate

Control ID - 45199: Ensure that the Controller Manager --profiling argument is set to false

Control ID - 45200: Ensure that the Controller Manager --use-service-account-credentials argument is set to true

Control ID - 45201: Ensure that the Controller Manager --service-account-private-key-file argument is set as appropriate

Control ID - 45202: Ensure that the Controller Manager --root-ca-file argument is set as appropriate

Control ID - 45203: Ensure that the Controller Manager RotateKubeletServerCertificate argument is set to true

Control ID - 45204: Ensure that the Controller Manager --bind-address argument is set to 127.0.0.1

Control ID - 45205: Ensure that the Scheduler --profiling argument is set to false

Control ID - 45206: Ensure that the Scheduler --bind-address argument is set to 127.0.0.1

Control ID - 45207: Ensure that the --cert-file and --key-file arguments are set as appropriate

Control ID - 45208: Ensure that the --client-cert-auth argument is set to true

Control ID - 45209: Ensure that the --auto-tls argument is not set to true

Control ID - 45210: Ensure that the --peer-cert-file and --peer-key-file arguments are set as appropriate

Control ID - 45211: Ensure that the --peer-client-cert-auth argument is set to true

Control ID - 45212: Ensure that the --peer-auto-tls argument is not set to true

Control ID - 45213: Ensure that a unique Certificate Authority is used for etcd

Control ID - 45214: Ensure that a minimal audit policy is created

Control ID - 45215: Ensure that the audit policy covers key security concerns

Control ID - 45216: Ensure that the kubelet service file permissions are set to 600 or more restrictive

Control ID - 45217: Ensure that the kubelet service file ownership is set to root:root

Control ID - 45218: If proxy kubeconfig file exists ensure permissions are set to 600 or more restrictive

Control ID - 45219: If proxy kubeconfig file exists ensure ownership is set to root:root

Control ID - 45220: Ensure that the --kubeconfig kubelet.conf file permissions are set to 600 or more restrictive

Control ID - 45081: Ensure that the --kubeconfig kubelet.conf file ownership is set to root:root

Control ID - 45221: Ensure that the certificate authorities file permissions are set to 600 or more restrictive

Control ID - 45222: Ensure that the client certificate authorities file ownership is set to root:root

Control ID - 45223: If the kubelet config.yaml configuration file is being used validate permissions set to 600 or more restrictive

Control ID - 45082: If the kubelet config.yaml configuration file is being used validate file ownership is set to root:root

Control ID - 45083: Ensure that the --anonymous-auth argument is set to false

Control ID - 45084: Ensure that the --authorization-mode argument is not set to AlwaysAllow

Control ID - 45085: Ensure that the --client-ca-file argument is set as appropriate

Control ID - 45086: Verify that the --read-only-port argument is set to 0

Control ID - 45087: Ensure that the --streaming-connection-idle-timeout argument is not set to 0

Control ID - 45089: Ensure that the --make-iptables-util-chains argument is set to true

Control ID - 45090: Ensure that the --hostname-override argument is not set

Control ID - 45091: Ensure that the eventRecordQPS argument is set to a level which ensures appropriate event capture

Control ID - 45131: Ensure that the --tls-cert-file and --tls-private-key-file arguments are set as appropriate

Control ID - 45092: Ensure that the --rotate-certificates argument is not set to false

Control ID - 45093: Verify that the RotateKubeletServerCertificate argument is set to true

Control ID - 45224: Ensure that the Kubelet only makes use of Strong Cryptographic Ciphers

Control ID - 45094: Ensure that the cluster-admin role is only used where required

Control ID - 45095: Minimize access to secrets

Control ID - 45096: Minimize wildcard use in Roles and ClusterRoles

Control ID - 45097: Minimize access to create pods

Control ID - 45098: Ensure that default service accounts are not actively used

Control ID - 45099: Ensure that Service Account Tokens are only mounted where necessary

Control ID - 45132: Limit use of the Bind, Impersonate and Escalate permissions in the Kubernetes cluster

Control ID - 45225: Ensure that the cluster has at least one active policy control mechanism in place

Control ID - 45226: Minimize the admission of privileged containers

Control ID - 45227: Minimize the admission of containers wishing to share the host process ID namespace

Control ID - 45228: Minimize the admission of containers wishing to share the host IPC namespace

Control ID - 45229: Minimize the admission of containers wishing to share the host network namespace

Control ID - 45230: Minimize the admission of containers with allowPrivilegeEscalation

Control ID - 45231: Minimize the admission of root containers

Control ID - 45232: Minimize the admission of containers with the NET_RAW capability

Control ID - 45233: Minimize the admission of containers with added capabilities

Control ID - 45100: Minimize the admission of containers with capabilities assigned

Control ID - 45234: Minimize the admission of Windows HostProcess Containers

Control ID - 45235: Minimize the admission of HostPath volumes

Control ID - 45236: Minimize the admission of containers which use HostPorts

Control ID - 45101: Ensure that the CNI in use supports Network Policies

Control ID - 45102: Ensure that all Namespaces have Network Policies defined

Control ID - 45103: Prefer using secrets as files over secrets as environment variables

Control ID - 45104: Consider external secret storage

Control ID - 45105: Create administrative boundaries between resources using namespaces

Control ID - 45237: Ensure that the seccomp profile is set to docker/default in your pod definitions

Control ID - 45106: Apply Security Context to Your Pods and Containers

Control ID - 45107: The default namespace should not be used

Control ID - 45238: Ensure that a limit is set on pod PIDs

Control ID - 45239: Ensure that the kube-proxy metrics service is bound to localhost

Control ID - 45146: Ensure that the API server pod specification file permissions are set to 600 or more restrictive

Control ID - 45147: Ensure that the API server pod specification file ownership is set to root:root

Control ID - 45148: Ensure that the controller manager pod specification file permissions are set to 600 or more restrictive

Control ID - 45149: Ensure that the controller manager pod specification file ownership is set to root:root

Control ID - 45150: Ensure that the scheduler pod specification file permissions are set to 600 or more restrictive

Control ID - 45151: Ensure that the scheduler pod specification file ownership is set to root:root

Control ID - 45152: Ensure that the etcd pod specification file permissions are set to 600 or more restrictive

Control ID - 45153: Ensure that the etcd pod specification file ownership is set to root:root

Control ID - 45154: Ensure that the Container Network Interface file permissions are set to 600 or more restrictive

Control ID - 45155: Ensure that the Container Network Interface file ownership is set to root:root

Control ID - 45156: Ensure that the etcd data directory permissions are set to 700 or more restrictive

Control ID - 45157: Ensure that the etcd data directory ownership is set to etcd:etcd

Control ID - 45158: Ensure that the admin.conf file permissions are set to 600

Control ID - 45159: Ensure that the admin.conf file ownership is set to root:root

Control ID - 45160: Ensure that the scheduler.conf file permissions are set to 600 or more restrictive

Control ID - 45161: Ensure that the scheduler.conf file ownership is set to root:root

Control ID - 45162: Ensure that the controller-manager.conf file permissions are set to 600 or more restrictive

Control ID - 45163: Ensure that the controller-manager.conf file ownership is set to root:root

Control ID - 45164: Ensure that the Kubernetes PKI directory and file ownership is set to root:root

Control ID - 45165: Ensure that the Kubernetes PKI certificate file permissions are set to 600 or more restrictive

Control ID - 45166: Ensure that the Kubernetes PKI key file permissions are set to 600

Control ID - 45167: Ensure that the API Server --anonymous-auth argument is set to false

Control ID - 45168: Ensure that the API Server --token-auth-file parameter is not set

Control ID - 45169: Ensure that the API Server --DenyServiceExternalIPs is not set

Control ID - 45170: Ensure that the API Server --kubelet-client-certificate and --kubelet-client-key arguments are set as appropriate

Control ID - 45171: Ensure that the API Server --kubelet-certificate-authority argument is set as appropriate

Control ID - 45172: Ensure that the API Server --authorization-mode argument is not set to AlwaysAllow

Control ID - 45173: Ensure that the API Server --authorization-mode argument includes Node

Control ID - 45174: Ensure that the API Server --authorization-mode argument includes RBAC

Control ID - 45175: Ensure that the admission control plugin EventRateLimit is set

Control ID - 45176: Ensure that the admission control plugin AlwaysAdmit is not set

Control ID - 45177: Ensure that the admission control plugin AlwaysPullImages is set

Control ID - 45179: Ensure that the admission control plugin ServiceAccount is set

Control ID - 45180: Ensure that the admission control plugin NamespaceLifecycle is set

Control ID - 45181: Ensure that the admission control plugin NodeRestriction is set

Control ID - 45183: Ensure that the API Server --profiling argument is set to false

Control ID - 45184: Ensure that the API Server --audit-log-path argument is set

Control ID - 45185: Ensure that the API Server --audit-log-maxage argument is set to 30 or as appropriate

Control ID - 45186: Ensure that the API Server --audit-log-maxbackup argument is set to 10 or as appropriate

Control ID - 45187: Ensure that the API Server --audit-log-maxsize argument is set to 100 or as appropriate

Control ID - 45188: Ensure that the API Server --request-timeout argument is set as appropriate

Control ID - 45189: Ensure that the API Server --service-account-lookup argument is set to true

Control ID - 45190: Ensure that the API Server --service-account-key-file argument is set as appropriate

Control ID - 45191: Ensure that the API Server --etcd-certfile and --etcd-keyfile arguments are set as appropriate

Control ID - 45192: Ensure that the API Server --tls-cert-file and --tls-private-key-file arguments are set as appropriate

Control ID - 45193: Ensure that the API Server --client-ca-file argument is set as appropriate

Control ID - 45194: Ensure that the API Server --etcd-cafile argument is set as appropriate

Control ID - 45195: Ensure that the API Server --encryption-provider-config argument is set as appropriate

Control ID - 45196: Ensure that encryption providers are appropriately configured

Control ID - 45197: Ensure that the API Server only makes use of Strong Cryptographic Ciphers

Control ID - 45241: Ensure that the --service-account-extend-token-expiration parameter is set to false

Control ID - 45198: Ensure that the Controller Manager --terminated-pod-gc-threshold argument is set as appropriate

Control ID - 45199: Ensure that the Controller Manager --profiling argument is set to false

Control ID - 45200: Ensure that the Controller Manager --use-service-account-credentials argument is set to true

Control ID - 45201: Ensure that the Controller Manager --service-account-private-key-file argument is set as appropriate

Control ID - 45202: Ensure that the Controller Manager --root-ca-file argument is set as appropriate

Control ID - 45203: Ensure that the Controller Manager RotateKubeletServerCertificate argument is set to true

Control ID - 45204: Ensure that the Controller Manager --bind-address argument is set to 127.0.0.1

Control ID - 45205: Ensure that the Scheduler --profiling argument is set to false

Control ID - 45206: Ensure that the Scheduler --bind-address argument is set to 127.0.0.1

Control ID - 45207: Ensure that the --cert-file and --key-file arguments are set as appropriate

Control ID - 45208: Ensure that the --client-cert-auth argument is set to true

Control ID - 45209: Ensure that the --auto-tls argument is not set to true

Control ID - 45210: Ensure that the --peer-cert-file and --peer-key-file arguments are set as appropriate

Control ID - 45211: Ensure that the --peer-client-cert-auth argument is set to true

Control ID - 45212: Ensure that the --peer-auto-tls argument is not set to true

Control ID - 45213: Ensure that a unique Certificate Authority is used for etcd

Control ID - 45213: Ensure that a unique Certificate Authority is used for etcd

Control ID - 45214: Ensure that a minimal audit policy is created

Control ID - 45215: Ensure that the audit policy covers key security concerns

Control ID - 45216: Ensure that the kubelet service file permissions are set to 600 or more restrictive

Control ID - 45217: Ensure that the kubelet service file ownership is set to root:root

Control ID - 45218: If proxy kubeconfig file exists ensure permissions are set to 600 or more restrictive

Control ID - 45219: If proxy kubeconfig file exists ensure ownership is set to root:root

Control ID - 45220: Ensure that the --kubeconfig kubelet.conf file permissions are set to 600 or more restrictive

Control ID - 45081: Ensure that the --kubeconfig kubelet.conf file ownership is set to root:root

Control ID - 45221: Ensure that the certificate authorities file permissions are set to 600 or more restrictive

Control ID - 45222: Ensure that the client certificate authorities file ownership is set to root:root

Control ID - 45223: If the kubelet config.yaml configuration file is being used validate permissions set to 600 or more restrictive

Control ID - 45082: If the kubelet config.yaml configuration file is being used validate file ownership is set to root:root

Control ID - 45083: Ensure that the --anonymous-auth argument is set to false

Control ID - 45084: Ensure that the --authorization-mode argument is not set to AlwaysAllow

Control ID - 45085: Ensure that the --client-ca-file argument is set as appropriate

Control ID - 45086: Verify that the --read-only-port argument is set to 0

Control ID - 45087: Ensure that the --streaming-connection-idle-timeout argument is not set to 0

Control ID - 45089: Ensure that the --make-iptables-util-chains argument is set to true

Control ID - 45090: Ensure that the --hostname-override argument is not set

Control ID - 45091: Ensure that the eventRecordQPS argument is set to a level which ensures appropriate event capture

Control ID - 45131: Ensure that the --tls-cert-file and --tls-private-key-file arguments are set as appropriate

Control ID - 45092: Ensure that the --rotate-certificates argument is not set to false

Control ID - 45093: Verify that the RotateKubeletServerCertificate argument is set to true

Control ID - 45224: Ensure that the Kubelet only makes use of Strong Cryptographic Ciphers

Control ID - 45238: Ensure that a limit is set on pod PIDs

Control ID - 45242: Ensure that the --seccomp-default parameter is set to true

Control ID - 45243: Ensure that the --IPAddressDeny is set to any

Control ID - 45239: Ensure that the kube-proxy metrics service is bound to localhost

Control ID - 45094: Ensure that the cluster-admin role is only used where required

Control ID - 45095: Minimize access to secrets

Control ID - 45096: Minimize wildcard use in Roles and ClusterRoles

Control ID - 45097: Minimize access to create pods

Control ID - 45098: Ensure that default service accounts are not actively used

Control ID - 45099: Ensure that Service Account Tokens are only mounted where necessary

Control ID - 45132: Limit use of the Bind, Impersonate and Escalate permissions in the Kubernetes cluster

Control ID - 45225: Ensure that the cluster has at least one active policy control mechanism in place

Control ID - 45226: Minimize the admission of privileged containers

Control ID - 45227: Minimize the admission of containers wishing to share the host process ID namespace

Control ID - 45228: Minimize the admission of containers wishing to share the host IPC namespace

Control ID - 45229: Minimize the admission of containers wishing to share the host network namespace

Control ID - 45230: Minimize the admission of containers with allowPrivilegeEscalation

Control ID - 45231: Minimize the admission of root containers

Control ID - 45232: Minimize the admission of containers with the NET_RAW capability

Control ID - 45233: Minimize the admission of containers with added capabilities

Control ID - 45100: Minimize the admission of containers with capabilities assigned

Control ID - 45234: Minimize the admission of Windows HostProcess Containers

Control ID - 45235: Minimize the admission of HostPath volumes

Control ID - 45236: Minimize the admission of containers which use HostPorts

Control ID - 45101: Ensure that the CNI in use supports Network Policies

Control ID - 45102: Ensure that all Namespaces have Network Policies defined

Control ID - 45103: Prefer using secrets as files over secrets as environment variables

Control ID - 45104: Consider external secret storage

Control ID - 45105: Create administrative boundaries between resources using namespaces

Control ID - 45237: Ensure that the seccomp profile is set to docker/default in your pod definitions

Control ID - 45106: Apply Security Context to Your Pods and Containers

Control ID - 45107: The default namespace should not be used

Control ID - 45001: Prevent containers from allowing command execution

Control ID - 45003: Roles with delete capabilities

Control ID - 45005: Non-root containers

Control ID - 45006: Access Kubernetes dashboard

Control ID - 45007: List Kubernetes secrets

Control ID - 45008: Allow privilege escalation

Control ID - 45009: Immutable container filesystem

Control ID - 45010: Configured readiness probe

Control ID - 45011: Mount service principal

Control ID - 45014: Ingress and Egress blocked

Control ID - 45015: Delete Kubernetes events

Control ID - 45016: Automatic mapping of service account

Control ID - 45017: Administrative Roles

Control ID - 45018: Validate admission controller (validating)

Control ID - 45019: Host PID/IPC privileges

Control ID - 45021: HostNetwork access

Control ID - 45022: SSH server running inside container

Control ID - 45023: Container hostPort

Control ID - 45024: Writable hostPath mount

Control ID - 45026: HostPath mount

Control ID - 45027: Network mapping

Control ID - 45029: Cluster internal networking

Control ID - 45030: Linux hardening

Control ID - 45031: Configured liveness probe

Control ID - 45032: Privileged container

Control ID - 45035: Pods in default namespace

Control ID - 45036: Sudo in container entrypoint

Control ID - 45037: Portforwarding privileges

Control ID - 45038: No impersonation

Control ID - 45042: Disable anonymous access to Kubelet service

Control ID - 45043: Enforce Kubelet client TLS authentication

Control ID - 45044: Naked pods

Control ID - 45045: Container runtime socket mounted

Control ID - 45046: Image pull policy on latest tag

Control ID - 45054: Anonymous user has RoleBinding

Control ID - 45055: system:authenticated user has elevated roles

Control ID - 45056: Ensure CPU limits are set

Control ID - 45057: Ensure memory limits are set

Control ID - 45060: Check if signature exists

Control ID - 45061: Missing network policy

Control ID - 45062: External facing

Control ID - 45063: Deprecated Kubernetes image registry

Control ID - 45064: Ensure CPU requests are set

Control ID - 45065: Ensure memory requests are set

Control ID - 45066: CoreDNS poisoning

Control ID - 45067: Workload with secret access

Control ID - 45068: Workload with PVC access

Control ID - 45069: Workload with ConfigMap access

Control ID - 45070: Workload with credential access

Control ID - 45071: ServiceAccount token mounted

Control ID - 45072: PersistentVolume without encryption

Control ID - 45073: Workload with cluster takeover roles

Control ID - 45074: Workload with administrative roles

Control ID - 45075: Outdated Kubernetes version

Control ID - 45076: Exposure to the internet via the Gateway API

Control ID - 45077: Verify Authenticated Service

Control ID - 45078: Ingress uses TLS

Control ID - 45146: Ensure that the API server pod specification file permissions are set to 600 or more restrictive

Control ID - 45147: Ensure that the API server pod specification file ownership is set to root:root

Control ID - 45148: Ensure that the controller manager pod specification file permissions are set to 600 or more restrictive

Control ID - 45149: Ensure that the controller manager pod specification file ownership is set to root:root

Control ID - 45150: Ensure that the scheduler pod specification file permissions are set to 600 or more restrictive

Control ID - 45151: Ensure that the scheduler pod specification file ownership is set to root:root

Control ID - 45152: Ensure that the etcd pod specification file permissions are set to 600 or more restrictive

Control ID - 45153: Ensure that the etcd pod specification file ownership is set to root:root

Control ID - 45160: Ensure that the scheduler.conf file permissions are set to 600 or more restrictive

Control ID - 45161: Ensure that the scheduler.conf file ownership is set to root:root

Control ID - 45162: Ensure that the controller-manager.conf file permissions are set to 600 or more restrictive

Control ID - 45163: Ensure that the controller-manager.conf file ownership is set to root:root

Control ID - 45084: Ensure that the --authorization-mode argument is not set to AlwaysAllow

Control ID - 45094: Ensure that the cluster-admin role is only used where required

Control ID - 45095: Minimize access to secrets

Control ID - 45096: Minimize wildcard use in Roles and ClusterRoles

Control ID - 45097: Minimize access to create pods

Control ID - 45098: Ensure that default service accounts are not actively used

Control ID - 45099: Ensure that Service Account Tokens are only mounted where necessary

Control ID - 45226: Minimize the admission of privileged containers

Control ID - 45227: Minimize the admission of containers wishing to share the host process ID namespace

Control ID - 45228: Minimize the admission of containers wishing to share the host IPC namespace

Control ID - 45229: Minimize the admission of containers wishing to share the host network namespace

Control ID - 45230: Minimize the admission of containers with allowPrivilegeEscalation

Control ID - 45231: Minimize the admission of root containers

Control ID - 45232: Minimize the admission of containers with the NET_RAW capability

Control ID - 45233: Minimize the admission of containers with added capabilities

Control ID - 45100: Minimize the admission of containers with capabilities assigned

Control ID - 45101: Ensure that the CNI in use supports Network Policies

Control ID - 45102: Ensure that all Namespaces have Network Policies defined

Control ID - 45103: Prefer using secrets as files over secrets as environment variables

Control ID - 45144: Consider external secret storage

Control ID - 45105: Create administrative boundaries between resources using namespaces

Control ID - 45237: Ensure that the seccomp profile is set to docker/default in your pod definitions

Control ID - 45106: Apply Security Context to Your Pods and Containers

Control ID - 45107: The default namespace should not be used

Control ID - 45244: Ensure that the kubeconfig file permissions are set to 600 or more restrictive

Control ID - 45245: Ensure that the kubeconfig file ownership is set to root:root

Control ID - 45246: Ensure that the --kubeconfig kubelet.conf file permissions are set to 644 or more restrictive

Control ID - 45247: Ensure that the kubelet --config configuration file has permissions set to 600 or more restrictive

Control ID - 45248: Ensure that the kubelet configuration file ownership is set to root:root

Control ID - 45249: Activate Garbage collection in OpenShift Container Platform 4, as appropriate