Checkmarx

KICS REPORT07/20/2023 23:46KICS.IO

KICS v1.7.4 Scanned

Privilege Escalation Allowed

Platform: Kubernetes **Category:** Insecure Configurations

Containers should not run with allowPrivilegeEscalation in order to prevent them from gaining more privileges than their parent processhttps://kubernetes.io/docs/tasks/configure-pod-container/security-context/

Results (3)

File: /charts/dapr/charts/dapr_operator/templates/dapr_operator_deployment.yaml Line 1

Expected: metadata.name={{dapr-operator}}.spec.template.spec.containers.name={{dapr-operator}}.securityContext.allowPrivilegeEscalation should be set and should be set to false
Found: metadata.name={{dapr-operator}}.spec.template.spec.containers.name={{dapr-operator}}.securityContext.allowPrivilegeEscalation is undefined

File: /charts/dapr/charts/dapr_sentry/templates/dapr_sentry_deployment.yaml Line 1

Expected: metadata.name={{dapr-sentry}}.spec.template.spec.containers.name={{dapr-sentry}}.securityContext.allowPrivilegeEscalation should be set and should be set to false
Found: metadata.name={{dapr-sentry}}.spec.template.spec.containers.name={{dapr-sentry}}.securityContext.allowPrivilegeEscalation is undefined

File: /charts/dapr/charts/dapr_sidecar_injector/templates/dapr_sidecar_injector_deployment.yaml Line 1

Expected: metadata.name={{dapr-sidecar-injector}}.spec.template.spec.containers.name={{dapr-sidecar-injector}}.securityContext.allowPrivilegeEscalation should be set and should be set to false
Found: metadata.name={{dapr-sidecar-injector}}.spec.template.spec.containers.name={{dapr-sidecar-injector}}.securityContext.allowPrivilegeEscalation is undefined

Role Binding To Default Service Account

Platform: Kubernetes **Category:** Insecure Defaults

No role nor cluster role should bind to a default service accounthttps://kubernetes.io/docs/tasks/configure-pod-container/configure-service-account/

Results (1)

File: /charts/dapr/charts/dapr_rbac/templates/secret-reader.yaml Line 26

Expected: subjects.kind=ServiceAccount.name should not be default **Found:** subjects.kind=ServiceAccount.name is default

```
25 {{- end }}
26subjects:
27- kind: ServiceAccount
```

Container Running With Low UID

Platform: Kubernetes **Category:** Best Practices

Check if containers are running with low UID, which might cause conflicts with the host's user table.https://kubernetes.io/docs/tasks/configure-pod-container/security-context/

Results (3)

File: /charts/dapr/charts/dapr_sentry/templates/dapr_sentry_deployment.yaml Line 1

Expected: metadata.name={{dapr-sentry}}.spec.template.spec.containers.name={{dapr-sentry}}.securityContext.runAsUser should be defined **Found:** metadata.name={{dapr-sentry}}.spec.template.spec.containers.name={{dapr-sentry}}.securityContext.runAsUser is undefined

File: /charts/dapr/charts/dapr_operator/templates/dapr_operator_deployment.yaml Line 1

Expected: metadata.name={{dapr-operator}}.spec.template.spec.containers.name={{dapr-operator}}.securityContext.runAsUser should be defined **Found:** metadata.name={{dapr-operator}}.spec.template.spec.containers.name={{dapr-operator}}.securityContext.runAsUser is undefined

File: /charts/dapr/charts/dapr_sidecar_injector/templates/dapr_sidecar_injector_deployment.yaml Line 1

Expected: metadata.name={{dapr-sidecar-injector}}.spec.template.spec.containers.name={{dapr-sidecar-injector}}.securityContext.runAsUser should be defined **Found:** metadata.name={{dapr-sidecar-injector}}.spec.template.spec.containers.name={{dapr-sidecar-injector}}.securityContext.runAsUser is undefined

NET_RAW Capabilities Not Being Dropped

Platform: Kubernetes **Category:** Insecure Configurations

Containers should drop 'ALL' or at least 'NET_RAW' capabilitieshttps://kubernetes.io/docs/tasks/configure-pod-container/security-context/

Results (3)

File: /charts/dapr/charts/dapr_operator/templates/dapr_operator_deployment.yaml Line 1

Expected: metadata.name={{dapr-operator}}.spec.template.spec.containers.name={{dapr-operator}}.securityContext.capabilities.drop should be defined **Found:** metadata.name={{dapr-operator}}.spec.template.spec.containers.name={{dapr-operator}}.securityContext.capabilities.drop is undefined

File: /charts/dapr/charts/dapr_sidecar_injector/templates/dapr_sidecar_injector_deployment.yaml Line 1

Expected: metadata.name={{dapr-sidecar-injector}}.spec.template.spec.containers.name={{dapr-sidecar-injector}}.securityContext.capabilities.drop should be defined **Found:** metadata.name={{dapr-sidecar-injector}}.spec.template.spec.containers.name={{dapr-sidecar-injector}}.securityContext.capabilities.drop is undefined

File: /charts/dapr/charts/dapr_sentry/templates/dapr_sentry_deployment.yaml Line 1

Expected: metadata.name={{dapr-sentry}}.spec.template.spec.containers.name={{dapr-sentry}}.securityContext.capabilities.drop should be defined **Found:** metadata.name={{dapr-sentry}}.spec.template.spec.containers.name={{dapr-sentry}}.securityContext.capabilities.drop is undefined

RBAC Roles with Read Secrets Permissions

Platform: Kubernetes **Category:** Access Control

Roles and ClusterRoles with get/watch/list RBAC permissions on Kubernetes secrets are dangerous and should be avoided. In case of compromise, attackers could abuse these roles to access sensitive data, such as passwords, tokens and keyshttps://kubernetes.io/docs/reference/access-authn-authz/rbac/

Results (4)

File: /charts/dapr/charts/dapr_rbac/templates/injector.yaml Line 53

Expected: metadata.name={{dapr-injector}}.rules[0] should not be granted read access to Secrets objects **Found:** metadata.name={{dapr-injector}}.rules[0] is granted read access (verbs: get) to Secrets objects

```
52 {{- end }}
53rules:
54 - apiGroups: [""]
```

File: /charts/dapr/charts/dapr_rbac/templates/secret-reader.yaml Line 12

Expected: metadata.name={{secret-reader}}.rules[0] should not be granted read access to Secrets objects **Found:** metadata.name={{secret-reader}}.rules[0] is granted read access (verbs: get) to Secrets objects

```
11 {{- end }}
12rules:
13- apiGroups: [""]
```

File: /charts/dapr/charts/dapr_rbac/templates/sentry.yaml Line 53

Expected: metadata.name={{dapr-sentry}}.rules[0] should not be granted read access to Secrets objects **Found:** metadata.name={{dapr-sentry}}.rules[0] is granted read access (verbs: get, update) to Secrets objects

```
52 {{- end }}
53rules:
54 - apiGroups: [""]
```

File: /charts/dapr/charts/dapr_rbac/templates/operator.yaml Line 19

Expected: metadata.name={{dapr-operator-admin}}.rules[8] should not be granted read access to Secrets objects **Found:** metadata.name={{dapr-operator-admin}}.rules[8] is granted read access (verbs: get, list, watch) to Secrets objects

```
18 {{- end }}
19rules:
20 - apiGroups: ["apiextensions.k8s.io"]
```

Seccomp Profile Is Not Configured

Platform: Kubernetes **Category:** Insecure Configurations

Containers should be configured with a secure Seccomp profile to restrict potentially dangerous syscallshttps://kubernetes.io/docs/tutorials/security/seccomp/#create-pod-that-uses-the-container-runtime-default-seccomp-profile

Results (3)

File: /charts/dapr/charts/dapr_sentry/templates/dapr_sentry_deployment.yaml Line 1

Expected: metadata.name={{dapr-sentry}}.spec.template.spec.containers.name={{dapr-sentry}}.securityContext.seccompProfile.type should be defined **Found:** metadata.name={{dapr-sentry}}.spec.template.spec.containers.name={{dapr-sentry}}.securityContext.seccompProfile.type is undefined

File: /charts/dapr/charts/dapr_operator/templates/dapr_operator_deployment.yaml Line 1

Expected: metadata.name={{dapr-operator}}.spec.template.spec.containers.name={{dapr-operator}}.securityContext.seccompProfile.type should be defined **Found:** metadata.name={{dapr-operator}}.spec.template.spec.containers.name={{dapr-operator}}.securityContext.seccompProfile.type is undefined

File: /charts/dapr/charts/dapr_sidecar_injector/templates/dapr_sidecar_injector_deployment.yaml Line 1

Expected: metadata.name={{dapr-sidecar-injector}}.spec.template.spec.containers.name={{dapr-sidecar-injector}}.securityContext.seccompProfile.type should be defined **Found:** metadata.name={{dapr-sidecar-injector}}.spec.template.spec.containers.name={{dapr-sidecar-injector}}.securityContext.seccompProfile.type is undefined

Service Account Token Automount Not Disabled

Platform: Kubernetes **Category:** Insecure Defaults

Service Account Tokens are automatically mounted even if not necessaryhttps://kubernetes.io/docs/tasks/configure-pod-container/configure-service-account/#use-the-default-service-account-to-access-the-api-server

Results (3)

File: /charts/dapr/charts/dapr_sentry/templates/dapr_sentry_deployment.yaml Line 1

Expected: metadata.name={{dapr-sentry}}.spec.template.spec.automountServiceAccountToken should be defined and set to false **Found:** metadata.name={{dapr-sentry}}.spec.template.spec.automountServiceAccountToken is undefined

File: /charts/dapr/charts/dapr_operator/templates/dapr_operator_deployment.yaml Line 1

Expected: metadata.name={{dapr-operator}}.spec.template.spec.automountServiceAccountToken should be defined and set to false **Found:** metadata.name={{dapr-operator}}.spec.template.spec.automountServiceAccountToken is undefined

File: /charts/dapr/charts/dapr_sidecar_injector/templates/dapr_sidecar_injector_deployment.yaml Line 1

Expected: metadata.name={{dapr-sidecar-injector}}.spec.template.spec.automountServiceAccountToken should be defined and set to false **Found:** metadata.name={{dapr-sidecar-injector}}.spec.template.spec.automountServiceAccountToken is undefined

ServiceAccount Allows Access Secrets

Platform: Kubernetes **Category:** Secret Management

Roles and ClusterRoles when binded, should not use get, list or watch as verbshttps://kubernetes.io/docs/reference/access-authn-authz/rbac/

Results (4)

File: /charts/dapr/charts/dapr_rbac/templates/secret-reader.yaml Line 1

Expected: The metadata.name={{secret-reader}}.rules.verbs should not contain the following verbs: [["get"]] **Found:** The metadata.name={{secret-reader}}.rules.verbs contain the following verbs: [["get"]]

File: /charts/dapr/charts/dapr_rbac/templates/operator.yaml Line 1

Expected: The metadata.name={{dapr-operator-admin}}.rules.verbs should not contain the following verbs: [["get", "list", "watch"]] **Found:** The metadata.name={{dapr-operator-admin}}.rules.verbs contain the following verbs: [["get", "list", "watch"]]

File: /charts/dapr/charts/dapr_rbac/templates/injector.yaml Line 1

Expected: The metadata.name={{dapr-injector}}.rules.verbs should not contain the following verbs: [["get"]] **Found:** The metadata.name={{dapr-injector}}.rules.verbs contain the following verbs: [["get"]]

File: /charts/dapr/charts/dapr_rbac/templates/sentry.yaml Line 1

Expected: The metadata.name={{dapr-sentry}}.rules.verbs should not contain the following verbs: [["get", "update"]] **Found:** The metadata.name={{dapr-sentry}}.rules.verbs contain the following verbs: [["get", "update"]]

Using Unrecommended Namespace

Platform: Kubernetes **Category:** Insecure Configurations

Namespaces like 'default', 'kube-system' or 'kube-public' should not be usedhttps://kubernetes.io/docs/concepts/overview/working-with-objects/kubernetes-objects/

Results (23)

File: /charts/dapr/charts/dapr_sentry/templates/dapr_sentry_deployment.yaml Line 6

Expected: metadata.namespace should be defined and not null **Found:** metadata.namespace is undefined or null

```
5metadata:
6 name: dapr-trust-bundle
7 labels:
```

File: /charts/dapr/charts/dapr_operator/templates/dapr_operator_service.yaml Line 20

Expected: metadata.namespace should be defined and not null **Found:** metadata.namespace is undefined or null

```
19metadata:
20 name: dapr-webhook
21 labels:
```

File: /charts/dapr/charts/dapr_rbac/templates/injector.yaml Line 78

Expected: metadata.namespace should be defined and not null **Found:** metadata.namespace is undefined or null

```
77 apiGroup: rbac.authorization.k8s.io
78 kind: Role
79 name: dapr-injector
```

File: /charts/dapr/charts/dapr_config/templates/dapr_default_config.yaml Line 5

Expected: metadata.namespace should be defined and not null **Found:** metadata.namespace is undefined or null

```
4metadata:
5 name: {{ .Values.dapr_default_system_config_name }}
6 labels:
```

File: /charts/dapr/charts/dapr_rbac/templates/injector.yaml Line 1

Expected: metadata.namespace should be defined and not null **Found:** metadata.namespace is undefined or null

File: /charts/dapr/charts/dapr_operator/templates/dapr_operator_deployment.yaml Line 31

Expected: metadata.namespace should be defined and not null **Found:** metadata.namespace is undefined or null

```
30metadata:
31 name: dapr-webhook-ca
32 labels:
```

File: /charts/dapr/charts/dapr_rbac/templates/sentry.yaml Line 1

Expected: metadata.namespace should be defined and not null **Found:** metadata.namespace is undefined or null

File: /charts/dapr/charts/dapr_rbac/templates/placement.yaml Line 4

Expected: metadata.namespace should be defined and not null **Found:** metadata.namespace is undefined or null

```
3metadata:
4 name: dapr-placement
5 labels:
```

File: /charts/dapr/charts/dapr_rbac/templates/sentry.yaml Line 78

Expected: metadata.namespace should be defined and not null **Found:** metadata.namespace is undefined or null

```
77 apiGroup: rbac.authorization.k8s.io
78 kind: Role
79 name: dapr-sentry
```

File: /charts/dapr/charts/dapr_rbac/templates/operator.yaml Line 4

Expected: metadata.namespace should be defined and not null **Found:** metadata.namespace is undefined or null

```
3metadata:
4 name: dapr-operator
5 labels:
```

File: /charts/dapr/charts/dapr_rbac/templates/sentry.yaml Line 4

Expected: metadata.namespace should be defined and not null **Found:** metadata.namespace is undefined or null

```
3metadata:
4 name: dapr-sentry
5 labels:
```

File: /charts/dapr/charts/dapr_rbac/templates/secret-reader.yaml Line 1

Expected: 'metadata.namespace' should not be set to default, kube-system or kube-public **Found:** 'metadata.namespace' is set to default

File: /charts/dapr/charts/dapr_sidecar_injector/templates/dapr_sidecar_injector_service.yaml Line 4

Expected: metadata.namespace should be defined and not null **Found:** metadata.namespace is undefined or null

```
3kind: Service
4metadata:
5 name: dapr-sidecar-injector
```

File: /charts/dapr/charts/dapr_sidecar_injector/templates/dapr_sidecar_injector_webhook_config.yaml Line 14

Expected: metadata.namespace should be defined and not null **Found:** metadata.namespace is undefined or null

```
13metadata:
14 name: dapr-sidecar-injector-cert
15 labels:
```

File: /charts/dapr/charts/dapr_operator/templates/dapr_operator_deployment.yaml Line 13

Expected: metadata.namespace should be defined and not null **Found:** metadata.namespace is undefined or null

```
12metadata:
13 name: dapr-webhook-cert
14 labels:
```

File: /charts/dapr/charts/dapr_rbac/templates/secret-reader.yaml Line 1

Expected: 'metadata.namespace' should not be set to default, kube-system or kube-public **Found:** 'metadata.namespace' is set to default

File: /charts/dapr/charts/dapr_rbac/templates/operator.yaml Line 152

Expected: metadata.namespace should be defined and not null **Found:** metadata.namespace is undefined or null

```
151metadata:
152 name: dapr-operator
153 labels:
```

File: /charts/dapr/charts/dapr_operator/templates/dapr_operator_deployment.yaml Line 1

Expected: metadata.namespace should be defined and not null **Found:** metadata.namespace is undefined or null

File: /charts/dapr/charts/dapr_operator/templates/dapr_operator_service.yaml Line 1

Expected: metadata.namespace should be defined and not null **Found:** metadata.namespace is undefined or null

File: /charts/dapr/charts/dapr_sidecar_injector/templates/dapr_sidecar_injector_deployment.yaml Line 1

Expected: metadata.namespace should be defined and not null **Found:** metadata.namespace is undefined or null

File: /charts/dapr/charts/dapr_rbac/templates/injector.yaml Line 4

Expected: metadata.namespace should be defined and not null **Found:** metadata.namespace is undefined or null

```
3metadata:
4 name: dapr-injector
5 labels:
```

File: /charts/dapr/charts/dapr_sentry/templates/dapr_sentry_deployment.yaml Line 1

Expected: metadata.namespace should be defined and not null **Found:** metadata.namespace is undefined or null

File: /charts/dapr/charts/dapr_rbac/templates/operator.yaml Line 163

Expected: metadata.namespace should be defined and not null **Found:** metadata.namespace is undefined or null

```
162 apiGroup: rbac.authorization.k8s.io
163 kind: Role
164 name: dapr-operator
```

Container Requests Not Equal To It's Limits

Platform: Kubernetes **Category:** Resource Management

Containers must have the same resource requests set as limits. This is recommended to avoid resource DDoS of the node during spikes and means that 'requests.memory' and 'requests.cpu' must equal 'limits.memory' and 'limits.cpu', respectivelyhttps://kubernetes.io/docs/concepts/configuration/manage-resources-containers/

Results (6)

File: /charts/dapr/charts/dapr_operator/templates/dapr_operator_deployment.yaml Line 1

Expected: metadata.name={{dapr-operator}}.spec.template.spec.containers.name={{dapr-operator}}.resources.requests.memory is equal to resources.limits.memory **Found:** metadata.name={{dapr-operator}}.spec.template.spec.containers.name={{dapr-operator}}.resources.requests.memory is not equal to resources.limits.memory

File: /charts/dapr/charts/dapr_sentry/templates/dapr_sentry_deployment.yaml Line 114

Expected: metadata.name={{dapr-sentry}}.spec.template.spec.containers.name={{dapr-sentry}}.resources.requests.cpu is equal to resources.limits.cpu **Found:** metadata.name={{dapr-sentry}}.spec.template.spec.containers.name={{dapr-sentry}}.resources.requests.cpu is not equal to resources.limits.cpu

```
113{{- end }}
114 resources:
115{{ toYaml .Values.resources | indent 10 }}
```

File: /charts/dapr/charts/dapr_sidecar_injector/templates/dapr_sidecar_injector_deployment.yaml Line 184

Expected: metadata.name={{dapr-sidecar-injector}}.spec.template.spec.containers.name={{dapr-sidecar-injector}}.resources.requests.cpu is equal to resources.limits.cpu **Found:** metadata.name={{dapr-sidecar-injector}}.spec.template.spec.containers.name={{dapr-sidecar-injector}}.resources.requests.cpu is not equal to resources.limits.cpu

```
183{{- end }}
184 resources:
185{{ toYaml .Values.resources | indent 10 }}
```

File: /charts/dapr/charts/dapr_sidecar_injector/templates/dapr_sidecar_injector_deployment.yaml Line 1

Expected: metadata.name={{dapr-sidecar-injector}}.spec.template.spec.containers.name={{dapr-sidecar-injector}}.resources.requests.memory is equal to resources.limits.memory **Found:** metadata.name={{dapr-sidecar-injector}}.spec.template.spec.containers.name={{dapr-sidecar-injector}}.resources.requests.memory is not equal to resources.limits.memory

File: /charts/dapr/charts/dapr_operator/templates/dapr_operator_deployment.yaml Line 133

Expected: metadata.name={{dapr-operator}}.spec.template.spec.containers.name={{dapr-operator}}.resources.requests.cpu is equal to resources.limits.cpu **Found:**

metadata.name={{dapr-operator}}.spec.template.spec.containers.name={{dapr-operator}}.resources.requests.cpu is not equal to resources.limits.cpu

```
132{{- end }}
133 resources:
134{{ toYaml .Values.resources | indent 10 }}
```

File: /charts/dapr/charts/dapr_sentry/templates/dapr_sentry_deployment.yaml Line 1

Expected: metadata.name={{dapr-sentry}}.spec.template.spec.containers.name={{dapr-sentry}}.resources.requests.memory is equal to resources.limits.memory **Found:** metadata.name={{dapr-sentry}}.spec.template.spec.containers.name={{dapr-sentry}}.resources.requests.memory is not equal to resources.limits.memory

Deployment Has No PodAntiAffinity

Platform: Kubernetes **Category:** Resource Management

Check if Deployment resources don't have a podAntiAffinity policy, which prevents multiple pods from being scheduled on the same node.https://kubernetes.io/docs/concepts/scheduling-eviction/assign-pod-node/

Results (3)

File: /charts/dapr/charts/dapr_sidecar_injector/templates/dapr_sidecar_injector_deployment.yaml Line 1

Expected: 'spec.template.spec.affinity.podAntiAffinity.preferredDuringSchedulingIgnoredDuringExecution[%!s(int=0)].podAffinityTerm.topologyKey' should be set to 'kubernetes.io/hostname' **Found:** 'spec.template.spec.affinity.podAntiAffinity.preferredDuringSchedulingIgnoredDuringExecution[%!s(int=0)].podAffinityTerm.topologyKey' is invalid or undefined

File: /charts/dapr/charts/dapr_operator/templates/dapr_operator_deployment.yaml Line 1

Expected: 'spec.template.spec.affinity.podAntiAffinity.preferredDuringSchedulingIgnoredDuringExecution[%!s(int=0)].podAffinityTerm.topologyKey' should be set to 'kubernetes.io/hostname' **Found:** 'spec.template.spec.affinity.podAntiAffinity.preferredDuringSchedulingIgnoredDuringExecution[%!s(int=0)].podAffinityTerm.topologyKey' is invalid or undefined

File: /charts/dapr/charts/dapr_sentry/templates/dapr_sentry_deployment.yaml Line 1

Expected: 'spec.template.spec.affinity.podAntiAffinity.preferredDuringSchedulingIgnoredDuringExecution[%!s(int=0)].podAffinityTerm.topologyKey' should be set to 'kubernetes.io/hostname' **Found:** 'spec.template.spec.affinity.podAntiAffinity.preferredDuringSchedulingIgnoredDuringExecution[%!s(int=0)].podAffinityTerm.topologyKey' is invalid or undefined

Image Pull Policy Of The Container Is Not Set To Always

Platform: Kubernetes **Category:** Insecure Configurations

Image Pull Policy of the container must be defined and set to Alwayshttps://kubernetes.io/docs/concepts/containers/images/#updating-images

Results (3)

File: /charts/dapr/charts/dapr_sidecar_injector/templates/dapr_sidecar_injector_deployment.yaml Line 1

Expected: metadata.name={{dapr-sidecar-injector}}.spec.template.spec.containers.name={{dapr-sidecar-injector}}.imagePullPolicy should be set to 'Always' **Found:** metadata.name={{dapr-sidecar-injector}}.spec.template.spec.containers.name={{dapr-sidecar-injector}}.imagePullPolicy relies on mutable images in cache

File: /charts/dapr/charts/dapr_sentry/templates/dapr_sentry_deployment.yaml Line 1

Expected: metadata.name={{dapr-sentry}}.spec.template.spec.containers.name={{dapr-sentry}}.imagePullPolicy should be set to 'Always' **Found:** metadata.name={{dapr-sentry}}.spec.template.spec.containers.name={{dapr-sentry}}.imagePullPolicy relies on mutable images in cache

File: /charts/dapr/charts/dapr_operator/templates/dapr_operator_deployment.yaml Line 1

Expected: metadata.name={{dapr-operator}}.spec.template.spec.containers.name={{dapr-operator}}.imagePullPolicy should be set to 'Always' **Found:** metadata.name={{dapr-operator}}.spec.template.spec.containers.name={{dapr-operator}}.imagePullPolicy relies on mutable images in cache

Image Without Digest

Platform: Kubernetes **Category:** Insecure Configurations

Images should be specified together with their digests to ensure integrityhttps://kubernetes.io/docs/concepts/containers/images/#updating-images

Results (4)

File: /charts/dapr/charts/dapr_operator/templates/dapr_operator_deployment.yaml Line 1

Expected: metadata.name={{dapr-operator}}.spec.template.spec.containers.name={{dapr-operator}}.image should specify the image with a digest **Found:** metadata.name={{dapr-operator}}.spec.template.spec.containers.name={{dapr-operator}}.image does not include an image digest

File: /charts/dapr/charts/dapr_sidecar_injector/templates/dapr_sidecar_injector_deployment.yaml Line 1

Expected: metadata.name={{dapr-sidecar-injector}}.spec.template.spec.containers.name={{dapr-sidecar-injector}}.image should specify the image with a digest **Found:** metadata.name={{dapr-sidecar-injector}}.spec.template.spec.containers.name={{dapr-sidecar-injector}}.image does not include an image digest

File: /charts/dapr/charts/dapr_sentry/templates/dapr_sentry_deployment.yaml Line 1

Expected: metadata.name={{dapr-sentry}}.spec.template.spec.containers.name={{dapr-sentry}}.image should specify the image with a digest **Found:** metadata.name={{dapr-sentry}}.spec.template.spec.containers.name={{dapr-sentry}}.image does not include an image digest

Missing AppArmor Profile

Platform: Kubernetes **Category:** Access Control

Containers should be configured with an AppArmor profile to enforce fine-grained access control over low-level system resourceshttps://kubernetes.io/docs/tutorials/clusters/apparmor/

Results (4)

File: /charts/dapr/charts/dapr_sentry/templates/dapr_sentry_deployment.yaml Line 1

Expected: metadata.name={{dapr-sentry}}.spec.template.metadata.annotations should specify an AppArmor profile for container {{dapr-sentry}} **Found:** metadata.name={{dapr-sentry}}.spec.template.metadata.annotations does not specify an AppArmor profile for container {{dapr-sentry}}

File: /charts/dapr/charts/dapr_operator/templates/dapr_operator_deployment.yaml Line 1

Expected: metadata.name={{dapr-operator}}.spec.template.metadata.annotations should specify an AppArmor profile for container {{dapr-operator}} **Found:** metadata.name={{dapr-operator}}.spec.template.metadata.annotations does not specify an AppArmor profile for container {{dapr-operator}}

File: /charts/dapr/charts/dapr_sidecar_injector/templates/dapr_sidecar_injector_deployment.yaml Line 1

Expected: metadata.name={{dapr-sidecar-injector}}.spec.template.metadata.annotations should specify an AppArmor profile for container {{dapr-sidecar-injector}} **Found:** metadata.name={{dapr-sidecar-injector}}.spec.template.metadata.annotations does not specify an AppArmor profile for container {{dapr-sidecar-injector}}

No Drop Capabilities for Containers

Platform: Kubernetes **Category:** Best Practices

Sees if Kubernetes Drop Capabilities exists to ensure containers security contexthttps://kubernetes.io/docs/concepts/workloads/pods/init-containers/

Results (3)

File: /charts/dapr/charts/dapr_operator/templates/dapr_operator_deployment.yaml Line 1

Expected: metadata.name={{dapr-operator}}.spec.containers.name={{dapr-operator}}.securityContext.capabilities should be set **Found:** metadata.name={{dapr-operator}}.spec.containers.name={{dapr-operator}}.securityContext.capabilities is undefined

File: /charts/dapr/charts/dapr_sidecar_injector/templates/dapr_sidecar_injector_deployment.yaml Line 1

Expected: metadata.name={{dapr-sidecar-injector}}.spec.containers.name={{dapr-sidecar-injector}}.securityContext.capabilities should be set **Found:** metadata.name={{dapr-sidecar-injector}}.spec.containers.name={{dapr-sidecar-injector}}.securityContext.capabilities is undefined

File: /charts/dapr/charts/dapr_sentry/templates/dapr_sentry_deployment.yaml Line 1

Expected: metadata.name={{dapr-sentry}}.spec.containers.name={{dapr-sentry}}.securityContext.capabilities should be set **Found:** metadata.name={{dapr-sentry}}.spec.containers.name={{dapr-sentry}}.securityContext.capabilities is undefined

Pod or Container Without LimitRange

Platform: Kubernetes **Category:** Insecure Configurations

Each namespace should have a LimitRange policy associated to ensure that resource allocations of Pods, Containers and PersistentVolumeClaims do not exceed the defined boundarieshttps://kubernetes.io/docs/concepts/policy/limit-range/

Results (3)

File: /charts/dapr/charts/dapr_sentry/templates/dapr_sentry_deployment.yaml Line 1

Expected: metadata.name={{dapr-sentry}} has a 'LimitRange' policy associated **Found:** metadata.name={{dapr-sentry}} does not have a 'LimitRange' policy associated

File: /charts/dapr/charts/dapr_sidecar_injector/templates/dapr_sidecar_injector_deployment.yaml Line 1

Expected: metadata.name={{dapr-sidecar-injector}} has a 'LimitRange' policy associated **Found:** metadata.name={{dapr-sidecar-injector}} does not have a 'LimitRange' policy associated

File: /charts/dapr/charts/dapr_operator/templates/dapr_operator_deployment.yaml Line 1

Expected: metadata.name={{dapr-operator}} has a 'LimitRange' policy associated **Found:** metadata.name={{dapr-operator}} does not have a 'LimitRange' policy associated

Pod or Container Without ResourceQuota

Platform: Kubernetes **Category:** Insecure Configurations

Each namespace should have a ResourceQuota policy associated to limit the total amount of resources Pods, Containers and PersistentVolumeClaims can consumehttps://kubernetes.io/docs/concepts/policy/resource-quotas/

Results (3)

File: /charts/dapr/charts/dapr_sentry/templates/dapr_sentry_deployment.yaml Line 1

Expected: metadata.name={{dapr-sentry}} has a 'ResourceQuota' policy associated **Found:** metadata.name={{dapr-sentry}} does not have a 'ResourceQuota' policy associated

File: /charts/dapr/charts/dapr_sidecar_injector/templates/dapr_sidecar_injector_deployment.yaml Line 1

Expected: metadata.name={{dapr-sidecar-injector}} has a 'ResourceQuota' policy associated **Found:** metadata.name={{dapr-sidecar-injector}} does not have a 'ResourceQuota' policy associated

File: /charts/dapr/charts/dapr_operator/templates/dapr_operator_deployment.yaml Line 1

Expected: metadata.name={{dapr-operator}} has a 'ResourceQuota' policy associated **Found:** metadata.name={{dapr-operator}} does not have a 'ResourceQuota' policy associated

Root Container Not Mounted Read-only

Platform: Kubernetes **Category:** Build Process

Check if the root container filesystem is not being mounted read-only.https://kubernetes.io/docs/tasks/configure-pod-container/security-context/

Results (3)

File: /charts/dapr/charts/dapr_sidecar_injector/templates/dapr_sidecar_injector_deployment.yaml Line 1

Expected: metadata.name={{dapr-sidecar-injector}}.spec.template.spec.containers.name={{dapr-sidecar-injector}}.securityContext.readOnlyRootFilesystem should be set to true **Found:** metadata.name={{dapr-sidecar-injector}}.spec.template.spec.containers.name={{dapr-sidecar-injector}}.securityContext.readOnlyRootFilesystem is undefined

File: /charts/dapr/charts/dapr_operator/templates/dapr_operator_deployment.yaml Line 1

Expected: metadata.name={{dapr-operator}}.spec.template.spec.containers.name={{dapr-operator}}.securityContext.readOnlyRootFilesystem should be set to true **Found:** metadata.name={{dapr-operator}}.spec.template.spec.containers.name={{dapr-operator}}.securityContext.readOnlyRootFilesystem is undefined

File: /charts/dapr/charts/dapr_sentry/templates/dapr_sentry_deployment.yaml Line 1

Expected: metadata.name={{dapr-sentry}}.spec.template.spec.containers.name={{dapr-sentry}}.securityContext.readOnlyRootFilesystem should be set to true **Found:** metadata.name={{dapr-sentry}}.spec.template.spec.containers.name={{dapr-sentry}}.securityContext.readOnlyRootFilesystem is undefined

Service Does Not Target Pod

Platform: Kubernetes **Category:** Insecure Configurations

Service should Target a Podhttps://kubernetes.io/docs/concepts/services-networking/service/

Results (1)

File: /charts/dapr/charts/dapr_operator/templates/dapr_operator_service.yaml Line 27

Expected: metadata.name={{dapr-webhook}}.spec.ports.port={{443}} has a Pod port **Found:** metadata.name={{dapr-webhook}}.spec.ports.port={{443}} does not have a Pod port

```
26 ports:
27 - port: 443
28 targetPort: 19443
```

KICS is open and will always stay such. Both the scanning engine and the security queries are clear and open for the software development community.

Spread the love: