KubeArmorHostPolicy Spec Diagram

metadata — name: [policy name] — Mandatory

namespace: [namespace name] — No Namespace in the case of KubeArmorHostPolicy

spec

severity: [1-10]

tags: ["tag1", "tag2", ...]

message: "message here"

action: {Audit | Block}

Mandatory if these are not defined in each rule

nodeSelector — nodeSelector (not selector)

Mandatory — matchLabels — key=value
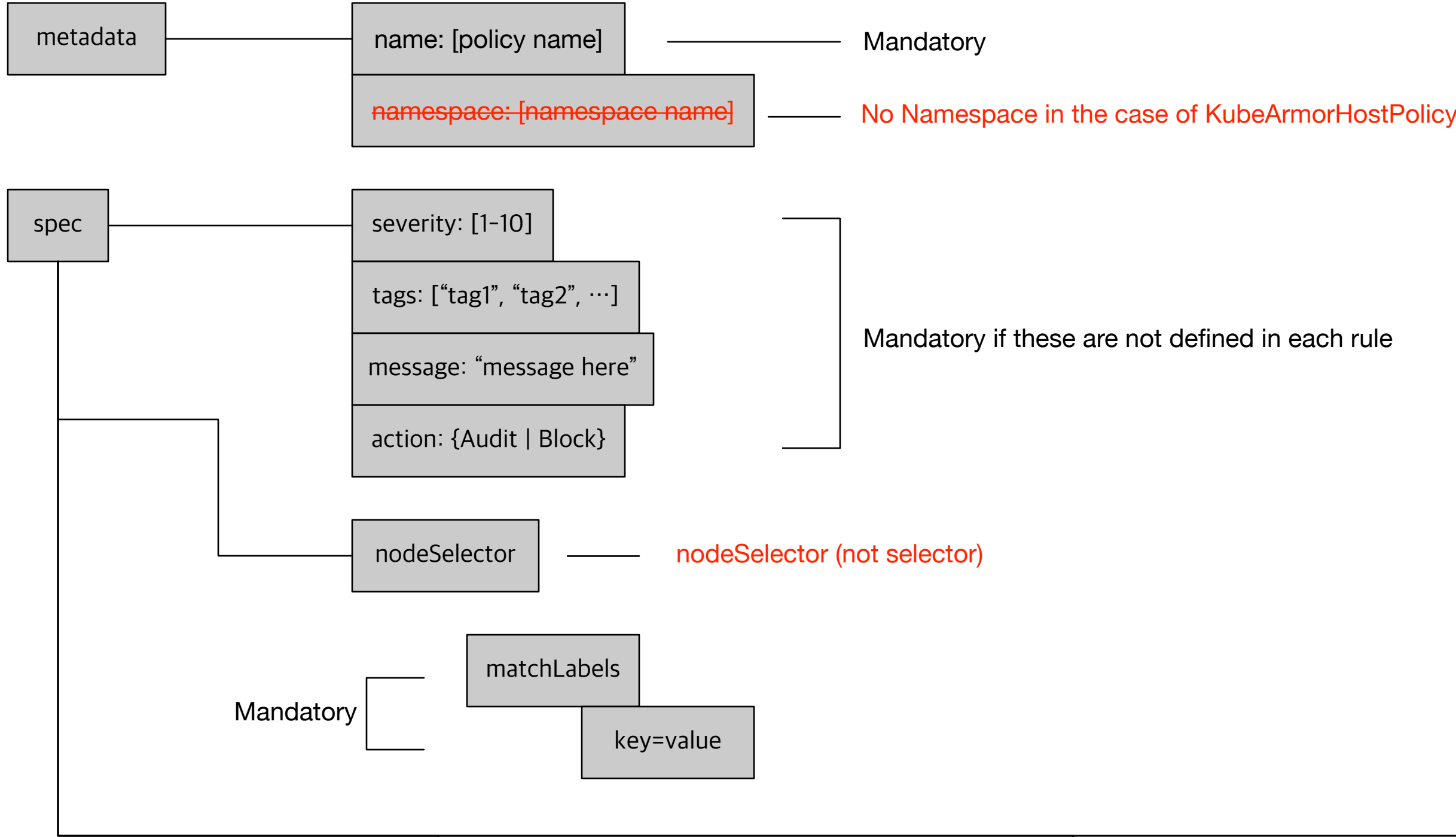
Key Difference between KubeArmorPolicy and KubeArmorHostPolicy

KubeArmorPolicy — action: {Allow | Audit | Block}
KubeArmorHostPolicy — action: {Allow | Audit | Block}

In the case that 'fromSource' is defined, then 'Allow' is available.

process

Optional

severity: [1-10]

tags: ["tag1", "tag2", ...]

message: "message here"

action: {Audit | Block}

matchPaths

path: [absolute executable path]

ownerOnly: [true|false]

fromSource

List — path: [absolute executable path]

List

Optional

severity: [1-10]

tags: ["tag1", "tag2", ...]

message: "message here"

action: {Audit | Block}

matchDirectories

dir: [absolute directory path]

recursive: [true|false]

ownerOnly: [true|false]

fromSource

List — path: [absolute executable path]

List

Optional

severity: [1-10]

tags: ["tag1", "tag2", ...]

message: "message here"

action: {Audit | Block}

matchPatterns

pattern: [regex pattern]

ownerOnly: [true|false]

List

Optional

severity: [1-10]

tags: ["tag1", "tag2", ...]

message: "message here"

action: {Audit | Block}

file

Optional

severity: [1-10]

tags: ["tag1", "tag2", ...]

message: "message here"

action: {Audit | Block}

matchPaths

path: [absolute file path]

readOnly: [true|false]

ownerOnly: [true|false]

fromSource

List — path: [absolute executable path]

List

Optional

severity: [1-10]

tags: ["tag1", "tag2", ...]

message: "message here"

action: {Audit | Block}

matchDirectories

dir: [absolute directory path]

recursive: [true|false]

readOnly: [true|false]

ownerOnly: [true|false]

fromSource

List — path: [absolute executable path]

List

Optional

severity: [1-10]

tags: ["tag1", "tag2", ...]

message: "message here"

action: {Audit | Block}

matchPatterns

pattern: [regex pattern]

readOnly: [true|false]

ownerOnly: [true|false]

List

Optional

severity: [1-10]

tags: ["tag1", "tag2", ...]

message: "message here"

action: {Audit | Block}

network

Optional

severity: [1-10]

tags: ["tag1", "tag2", ...]

message: "message here"

action: {Audit | Block}

matchProtocols

protocol: { tcp | udp | icmp }

fromSource

List — path: [absolute executable path]

List

Optional

severity: [1-10]

tags: ["tag1", "tag2", ...]

message: "message here"

action: {Audit | Block}

capabilities

Optional

severity: [1-10]

tags: ["tag1", "tag2", ...]

message: "message here"

action: {Audit | Block}

matchCapabilities

capability: { net_raw }

fromSource

List — path: [absolute executable path]

List

Optional

severity: [1-10]

tags: ["tag1", "tag2", ...]

message: "message here"

action: {Audit | Block}