ICN-MTSCN R5 Installation Guide

How to setup Kata in ICN

It is required to use Containerd as the Container Runtime Interface (CRI) into Kubernetes to be able to select Kata as a RuntimeClass. It won't work with Docker because it is not possible to change OCI runtimes dynamically using Docker. The R5 Secure Container release of ICN adds support for Containerd as a CRI.

When doing a containerized deployment of Kubernetes using the bpa-operator on the Jump server there is a ConfigMap of default values that is used by the installer. Users of ICN can change the values of the ConfigMap to control which CRI runtime is used, whether to enable testing, along with some other values. This file is in the ICN repo and is located at cmd/bpa-operator/deploy/kud-installer.yaml. In the bpa-operator folder there is a Makefile with a deploy option. The command make deploy will use kubectl to apply the bpa-operator along with the ConfigMap and other related service accounts and roles. Alternatively, you can run the kubectl commands directly to setup the operator and ConfigMap values. Even if the ConfigMap has already been deployed it is easy to update the values just by changing what is in kud-installer.yaml and then running the following command.

```
kubectl apply -f deploy/kud-installer.yaml
```

Once Kubernetes is deployed to each of the nodes and before any addons are installed there are some ansible scripts that will install Kata using kata-deploy. Kata artifacts will only be installed on nodes that jobs can be scheduled on. Typically this means that there won't be any Kata artifacts installed on the master node in a multi-node setup and will only be installed on the worker nodes.

Table 1: Default kud-installer.yaml ConfigMap values

Configuration Variable	Valid Values	Default Value
CONTAINER_RUNTIME	docker containerd	docker
KUD_DEBUG	<blank> true	<blank>
KUD_ENABLE_TESTS	true false	false
ENABLE_KATA_WEBHOOK	true false	false
KATA_WEBHOOK_RUNTIMECLASS	kata-clh kata-qemu	kata-clh

CONTAINER_RUNTIME

This is the Container Runtime Interface for Kubernetes. The default is to use Docker with no Kata support. If Containerd is chosen, then Kata will be installed as part of the cluster.

KUD_DEBUG

The default is to leave this blank and not enabled. If it is set to "true" then the ansible scripts that run will have "-vvv" (verbosity level of 3) enabled in the logging output.

KUD_ENABLE_TESTS

If this is set to "true" then some simple tests will be run to verify each addon was successfully installed. For the Kata tests, a simple pod will be started with the Cloud Hypervisor using the kata-clh RuntimeClass and another pod will be started with QEMU using the kata-qemu RuntimeClass. In addition, before the other plugins are tested, a Kata webhook will be installed into the cluster to mutate eligible pods to add in the Kata RuntimeClass to the Pod spec so that those pods are run more securely with Kata Containers.

ENABLE_KATA_WEBHOOK

The Kata webhook will mutate every eligible pod to use the Kata runtime. It is turned off by default because it is expected that users will want to specify which pods should run more securely with Kata containers and which ones should not. If KUD_ENABLE_TESTS is “true” and ENABLE_KATA_WEBHOOK is “false” then be aware that when the addons are tested the webhook will be installed during that time and uninstalled after all the tests successfully passed.

KATA_WEBHOOK_RUNTIMECLASS

This is the default hypervisor with its RuntimeClass settings that will be used by the webhook when it mutates pods to use the Kata runtime. The default is to use cloud-hypervisor (kata-clh) but QEMU (kata-qemu) is also supported.

How to use Kata with ICN

Using Kata in an ICN deployment is as simple as adding the RuntimeClass to each Pod spec. Below is a simple example showing how this is done for the cloud-hypervisor test pod.

Kata RuntimeClass example

```
kind: Pod

apiVersion: v1

metadata:

  name: kata-clh

spec:

  runtimeClassName: kata-clh

  containers:

    - name: busybox

      image: busybox

      imagePullPolicy: Always

      command: [ "sleep", "100000" ]
```

Alternatively, if the Kata webhook is enabled then all pods that are not privileged and do not have net=host will be mutated to run as a Kata Container using the hypervisor specified with KATA_WEBHOOK_RUNTIMECLASS.

Note: Please refer to the ICN README.md for further installation instructions.