
KubeCon
CloudNativeCon
North America 2022
BUILDING FOR THE ROAD AHEAD
DETROIT 2022
TiKV
TiKV
HELM

BUILDING FOR THE ROAD AHEAD

DETROIT 2022

Windows HostProcess Containers For Configuration And Beyond

James Sturtevant &
Mark Rossetti

Windows Debug


```
⎈ test-aks-13796-cluster in ~
❯
```

Windows HostProcess Containers

KubeCon | CloudNativeCon
North America 2022

BUILDING FOR THE ROAD AHEAD

DETROIT 2022

October 24-28, 2021

James Sturtevant
Software Engineer
Microsoft
@aspenwilder

Mark Rossetti
Software Engineer
Microsoft
[not on twitter]

Agenda

- Overview of HostProcess Containers
- Deployments in Action
- Demos
  - Restricting Node Access
  - Building HostProcess Containers
  - Collecting Events
  - Network Troubleshooting
- Additional Resources
- Q & A

What are HostProcess Containers?

HostProcess Containers

- Workloads are packaged / distributed / deployed as containers
- Container workload is run as a process directly on the host
  - Full access* to host's file-system, network stack, process space, etc
- Native support in Kubernetes / full support for:
  - Volume mounts
  - Resource limits
  - Metrics
  - Logging
  - ServiceAccount based cluster access
  - much more!

Motivation

- Provisioning / managing Windows nodes ~~is~~ was difficult.
- No standardization on how to run essential components like CNI solutions / kubeproxy / etc!

Before HostProcess Containers

- Difficult to deploy / manage
  - ✗ Custom PowerShell
  - ✗ Service helpers like nssm.exe
  - ✗ No (good) upgrade story
  - ✗ Required access to the nodes
- Difficult to monitor
  - ✗ No visibility
  - ✗ Required access to the nodes
  - ✗ No easy way to get logs

With HostProcess Containers

- Deploy as DaemonSet
  - ✓ Familiar install story
  - ✓ Runs as a container
  - ✓ Familiar upgrade story
  - ✓ Node access not required
- Monitor just like any other K8s workload
  - ✓ Visibility
  - ✓ Easily get logs

Support

- Beta in K8s v1.23, Stable in v1.26
- Currently containerd only!

BUILDING FOR THE ROAD AHEAD

DETROIT 2022

HostProcess Containers in Action

CNIs


```
securityContext:
       windowsOptions:
         hostProcess: true
         runAsUserName: "NT AUTHORITY\\system"
     hostNetwork: true
initContainers:
       - name: install-cni
         image: sigwindowstools/calico-install:v3.20.0-hostprocess
         args: ["calico/install.ps1"]
containers:
     - name: calico-node-startup
       image: sigwindowstools/calico-node:v3.20.0-hostprocess
       args: ["calico/node-service.ps1"]
       workingDir: "calico/"
     - name: calico-node-felix
       image: sigwindowstools/calico-node:v3.20.0-hostprocess
       args: ["calico/felix-service.ps1"]
       imagePullPolicy: Always
       workingDir: "calico/"
volumeMounts:
       - name: calico-config-windows
         mountPath: /etc/kube-calico-windows/
volumes:
     - name: calico-config-windows
       configMap:
         name: calico-config-windows
     # Used to install CNI.
     - name: cni-bin-dir
       hostPath:
         path: /opt/cni/bin
     - name: cni-net-dir
       hostPath:
         path: /etc/cni/net.d
```

```
securityContext:
       windowsOptions:
         hostProcess: true
         runAsUserName: "NT AUTHORITY\\system"
     hostNetwork: true
```

```
initContainers:
        - name: install-cni
          image: sigwindowstools/calico-install:v3.20.0-hostprocess
          args: ["calico/install.ps1"]
```

```
containers:
    - name: calico-node-startup
      image: sigwindowstools/calico-node:v3.20.0-hostprocess
      args: ["calico/node-service.ps1"]
      workingDir: "calico/"
    - name: calico-node-felix
      image: sigwindowstools/calico-node:v3.20.0-hostprocess
      args: ["calico/felix-service.ps1"]
      imagePullPolicy: Always
      workingDir: "calico/"
```

```
volumeMounts:
       - name: calico-config-windows
         mountPath: /etc/kube-calico-windows/
volumes:
     - name: calico-config-windows
       configMap:
         name: calico-config-windows
     # Used to install CNI.
     - name: cni-bin-dir
       hostPath:
         path: /opt/cni/bin
     - name: cni-net-dir
       hostPath:
         path: /etc/cni/net.d
```

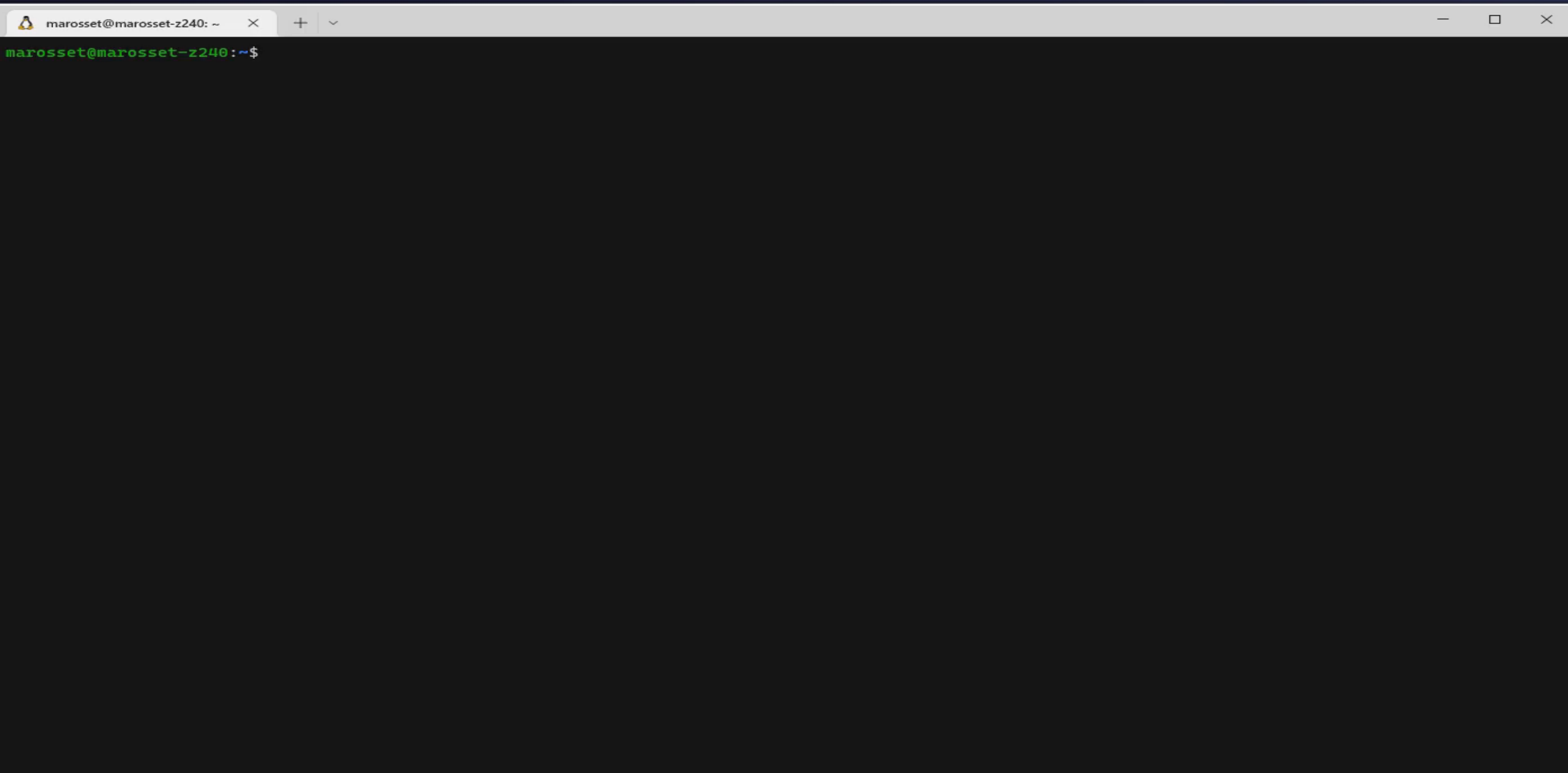
Kube-proxy


```
securityContext:
  windowsOptions:
    hostProcess: true
    runAsUserName: "NT AUTHORITY\\system"
hostNetwork: true
containers:
     - image: sigwindowstools/kube-proxy:v1.24.3-
calico-hostprocess
       args: ["kube-proxy/start.ps1"]
       workingDir: "kube-proxy/"
       name: kube-proxy
       env:
       - name: NODE_NAME
         valueFrom:
           fieldRef:
             apiVersion: v1
             fieldPath: spec.nodeName
       - name: POD_IP
         valueFrom:
           fieldRef:
             fieldPath: status.podIP
tolerations:
    - key: CriticalAddonsOnly
      operator: Exists
    - operator: Exists
updateStrategy:
  type: RollingUpdate
```

```
containers:
     - image: sigwindowstools/kube-proxy:v1.24.3-
calico-hostprocess
       args: ["kube-proxy/start.ps1"]
       workingDir: "kube-proxy/"
       name: kube-proxy
       env:
       - name: NODE_NAME
         valueFrom:
           fieldRef:
             apiVersion: v1
             fieldPath: spec.nodeName
       - name: POD_IP
         valueFrom:
           fieldRef:
             fieldPath: status.podIP
```

```
tolerations:
    - key: CriticalAddonsOnly
      operator: Exists
    - operator: Exists
updateStrategy:
  type: RollingUpdate
```

Security Options



HPC Base Image

- Can only be used with HostProcess containers
- Very small! ~25Kb
- Same image work on all Windows Server OS versions!!!
- Must use BuildKit to build images
- http://bit.ly/hpc-base-image (link to GH repo)

HPC Base Image - Demo

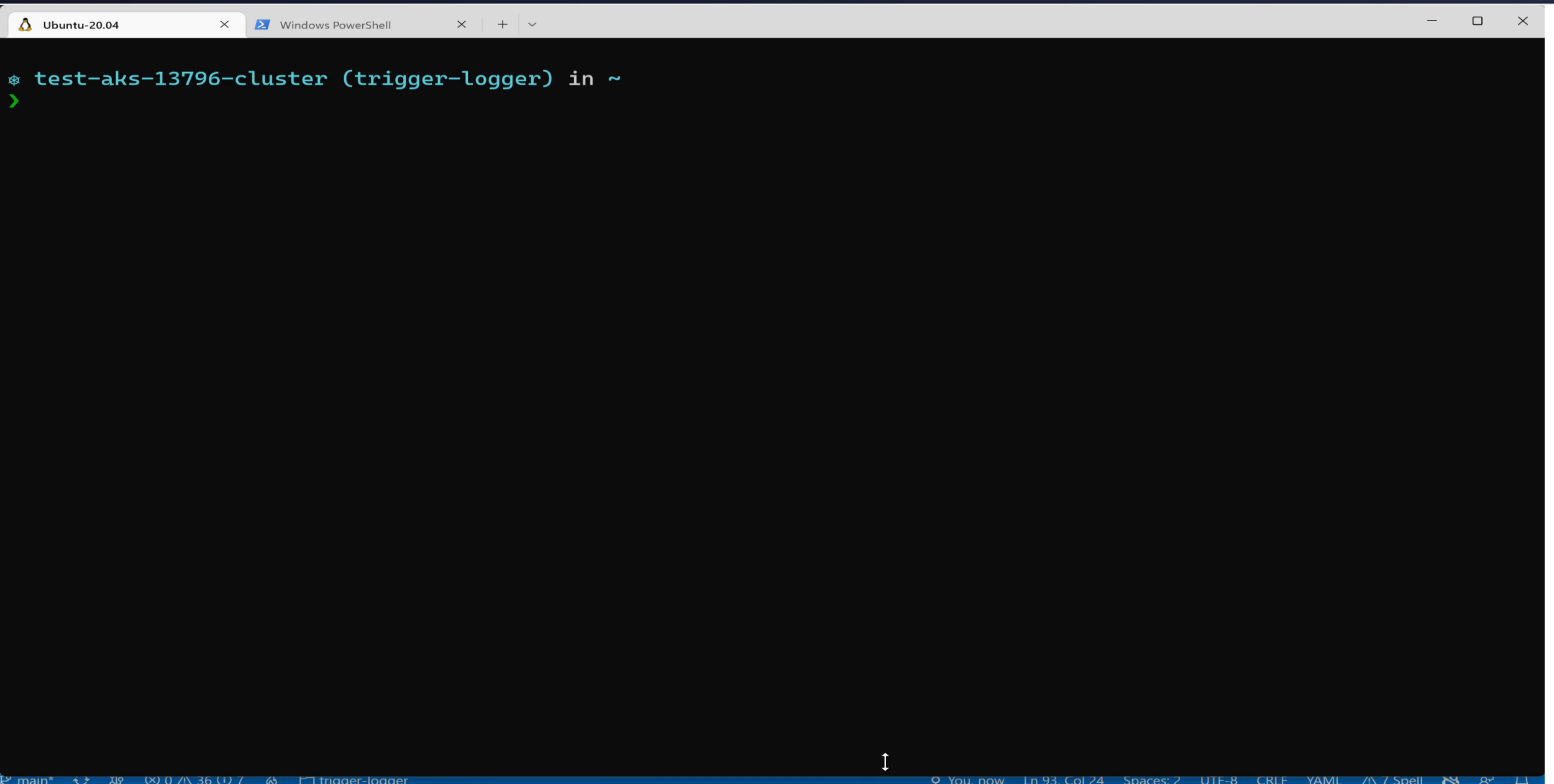
KubeCon CloudNativeCon North America 2022

```
marosset@marosset-z240:~/scratch/hpc$
```

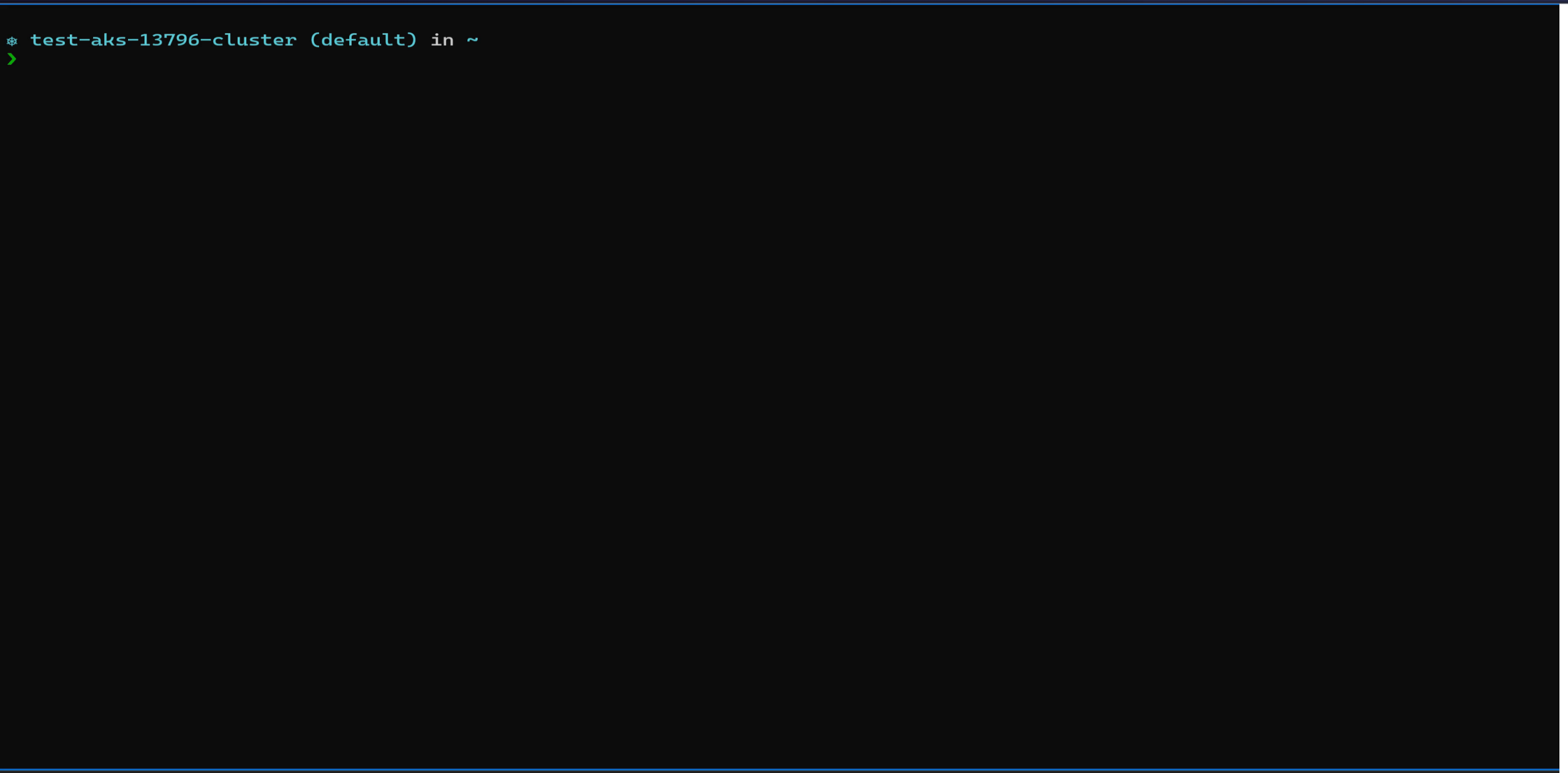
KubeCon | CloudNativeCon
North America 2022
BUILDING FOR THE ROAD AHEAD
DETROIT 2022

Collecting Events from the Node

Logging - Demo



Networking - Demo



Additional Resources

Projects to check out

- WCNspect
- Window-Debug image
- Trigger Logger
- EventFlow Logger
- CSI-proxy
- Kube-proxy
- Calico CNI
- Windows Exporter (Prometheus)
- KuReD
- Democratic-CSI
- More!

(Download slides for links)

Great way to contribute to new projects!

More SIG-Windows Talks

- **Windows Operational Readiness**
  Thursday - Oct 27th 3:25 PM EDT – Ambassador Ballroom (Room 360)
  https://sched.co/182FM

- **What's New With SIG-Windows**
  Thursday - Oct 27th 5:25 EDT – 142 ABC
  https://sched.co/182Oq

- **Lessons From Scheduling 20 Million Windows Containers a Month**
  Friday - Oct 28th 11:55 EDT – 250 ABC
  https://sched.co/182Ea

Resources

James Sturtevant
@jsturtevant [K8s Slack]
@jsturtevant [GitHub]
@aspenwilder [twitter]

Mark Rossetti
@Mark Rossetti [K8s Slack]
@marosset [GitHub]

KEP : https://bit.ly/k8s-hpc-kep

Docs: https://kubernetes.io/docs/tasks/configure-pod-container/create-hostprocess-pod/

Base Image: https://github.com/microsoft/windows-host-process-containers-base-image

Examples: https://github.com/kubernetes-sigs/sig-windows-tools/tree/master/hostprocess

---

SIG-Windows

- #sig-windows [K8s Slack]
- https://github.com/kubernetes/community/tree/master/sig-windows
- Community meetings every Tuesday @ 12:30 pm EST

Q & A

KubeCon | CloudNativeCon
North America 2022

BUILDING FOR THE ROAD AHEAD

DETROIT 2022

Please scan the QR Code above to
leave feedback on this session