Lesson 07 Demo 02

Working with Kubernetes Cluster Logging Architecture

Objective: To monitor and manage application logs within Kubernetes clusters by retrieving logs for specific pods and using log options to filter and manage log data

Tools required: kubeadm, kubectl, kubelet, and containerd

Prerequisites: A Kubernetes cluster (refer to Demo 01 from Lesson 01 for setting up a cluster)

Steps to be followed:

1. Retrieve log entries for a Kubernetes pod
2. Use the log options and switch information

Step 1: Retrieve log entries for a Kubernetes pod

1.1 To invoke the help menu, execute the following command:

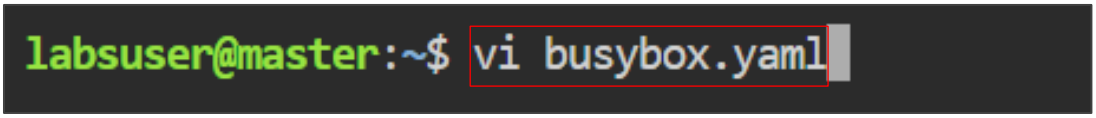
kubectl logs --help

```
labsuser@master:~$ kubectl logs --help
Print the logs for a container in a pod or specified resource. If the pod has only one container, the container name is
optional.

Examples:
  # Return snapshot logs from pod nginx with only one container
  kubectl logs nginx

  # Return snapshot logs from pod nginx with multi containers
  kubectl logs nginx --all-containers=true

  # Return snapshot logs from all containers in pods defined by label app=nginx
  kubectl logs -l app=nginx --all-containers=true

  # Return snapshot of previous terminated ruby container logs from pod web-1
  kubectl logs -p -c ruby web-1

  # Begin streaming the logs of the ruby container in pod web-1
  kubectl logs -f -c ruby web-1

  # Begin streaming the logs from all containers in pods defined by label app=nginx
  kubectl logs -f -l app=nginx --all-containers=true

  # Display only the most recent 20 lines of output in pod nginx
  kubectl logs --tail=20 nginx
```

```
    --since-time='':
        Only return logs after a specific date (RFC3339). Defaults to all logs. Only one of since-time / since may be
        used.

    --tail=-1:
        Lines of recent log file to display. Defaults to -1 with no selector, showing all log lines otherwise 10, if a
        selector is provided.

    --timestamps=false:
        Include timestamps on each line in the log output

Usage:
  kubectl logs [-f] [-p] (POD | TYPE/NAME) [-c CONTAINER] [options]

Use "kubectl options" for a list of global command-line options (applies to all commands).
labsuser@master:~$
```

1.2 Create a pod named **busybox** using the following command:

vi busybox.yaml



1.3 Enter the following code in **busybox.yaml** file:

```
apiVersion: v1
kind: Pod
metadata:
  name: counter
spec:
  containers:
  - name: count
    image: busybox:1.28
    args: [/bin/sh, -c,
          'i=0; while true; do echo "$i: $(date)"; i=$((i+1)); sleep 1; done']
```

```
apiVersion: v1
kind: Pod
metadata:
  name: counter
spec:
  containers:
  - name: count
    image: busybox:1.28
    args: [/bin/sh, -c,
            'i=0; while true; do echo "$i: $(date)"; i=$((i+1)); sleep 1; done']
~
~
~
~
~
~
~
~
~
~
~
~
~
~
:wq
```

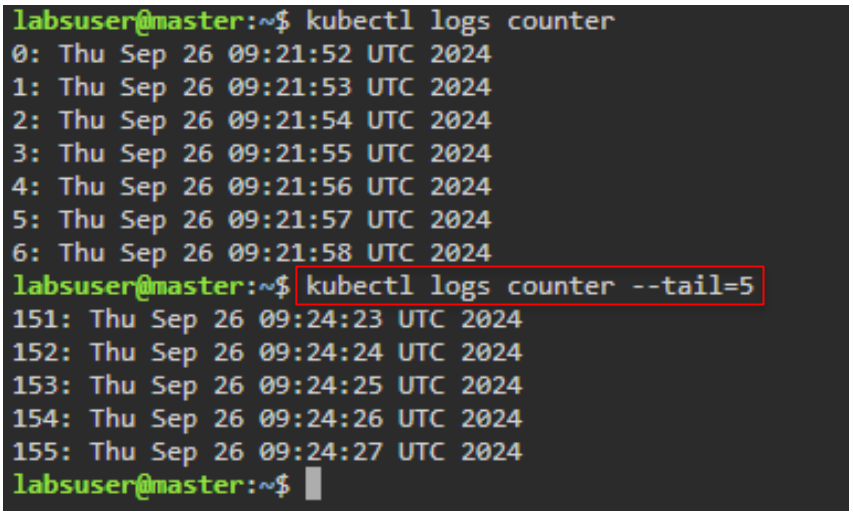
1.4 Deploy the YAML file and check its logs using the following commands:

kubectl apply -f busybox.yaml

kubectl logs counter

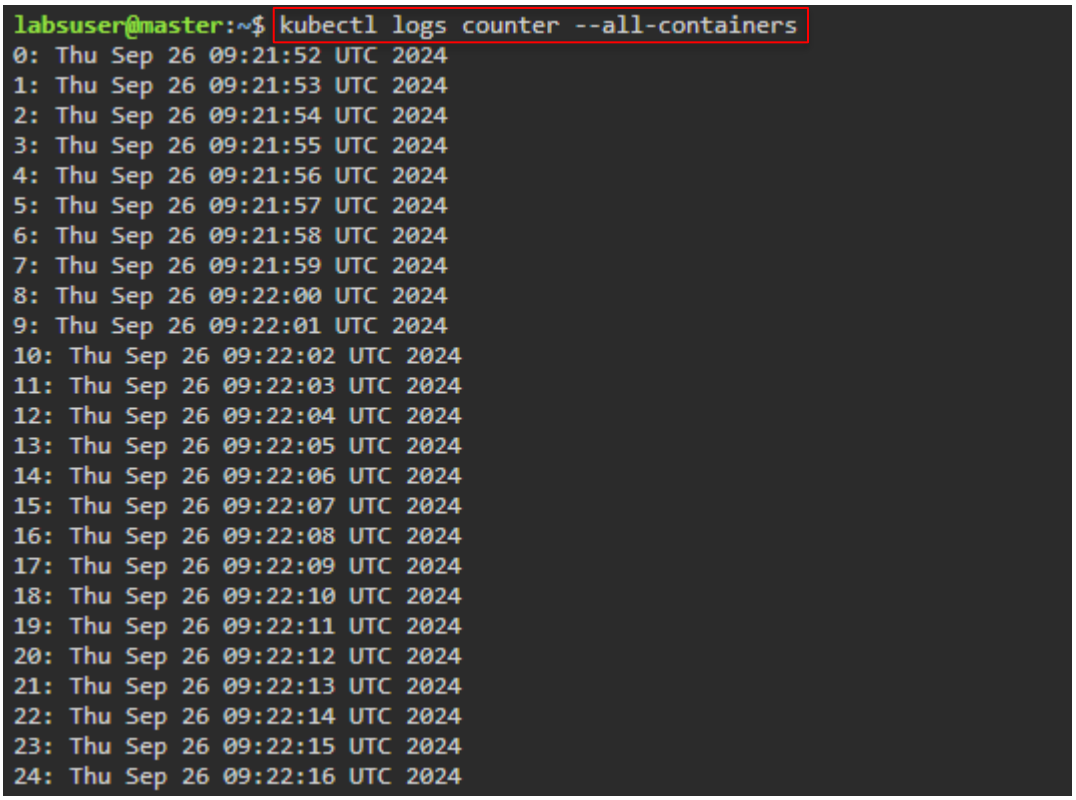
```
labsuser@master:~$ vi busybox.yaml
labsuser@master:~$ kubectl apply -f busybox.yaml
pod/counter created
labsuser@master:~$ kubectl logs counter
0: Thu Sep 26 09:21:52 UTC 2024
1: Thu Sep 26 09:21:53 UTC 2024
2: Thu Sep 26 09:21:54 UTC 2024
3: Thu Sep 26 09:21:55 UTC 2024
4: Thu Sep 26 09:21:56 UTC 2024
5: Thu Sep 26 09:21:57 UTC 2024
6: Thu Sep 26 09:21:58 UTC 2024
```

1.5 To retrieve the last five lines of the log, execute the following command:
kubectl logs counter --tail=5



Step 2: Use the log options and switch information

2.1 To obtain logs from all containers in a namespace, execute the following command:
kubectl logs counter --all-containers

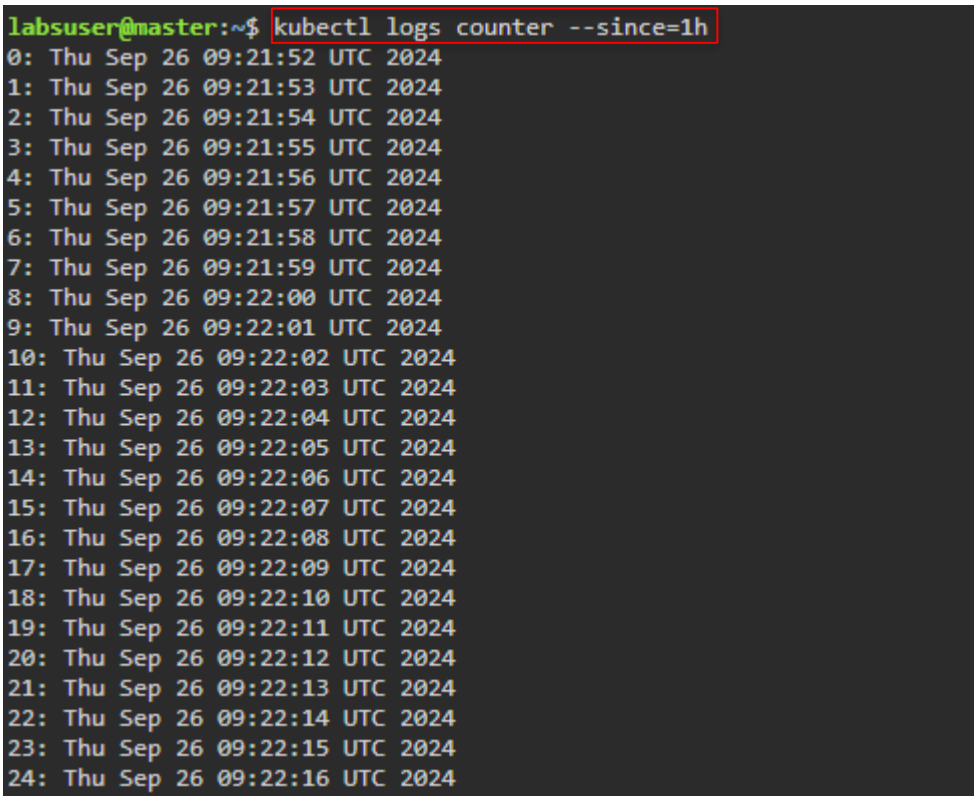


2.2 To get logs from a specific time range, use the following format:

kubectl logs counter --since=<timespan>

For example, to get logs from the past hour:

kubectl logs counter --since=1h



By following these steps, you have successfully obtained hands-on experience with Kubernetes logging and gained a deeper understanding of the cluster's logging architecture.