```
        kubectl delete -f $ns.configmap/$s && kubectl create -f $ns.configmap/$s
    done
done

kubectl --force --grace-period=0 delete pv $(kubectl get pv | grep -e
"image-manager-" -e "icp-mongodb-" -e "mariadb-" -e "logging-datanode-" -e
"kafka-" -e "zookeeper-" -e "minio-"  | awk '{print $1}')

kubectl patch pv $(kubectl get pv | grep Terminating | awk '{print $1}') -p
'{"metadata":{"finalizers":null}}'

kubectl delete pvc -n kube-system $(kubectl get pvc -n kube-system | grep -e
"image-manager-image-manager-" -e "mongodbdir-icp-mongodb-" -e
"mysqldata-mariadb-" -e "data-logging-elk-data-" -e "-vulnerability-advisor-" -e
"datadir-vulnerability-advisor-kafka-" -e
"datadir-vulnerability-advisor-zookeeper-" -e
"datadir-vulnerability-advisor-minio-" | awk '{print $1}')


echo "Done."
```

Alternatively download and run the script from the following link:

https://github.com/IBMRedbooks/SG248440-IBM-Cloud-Private-System-Administrator-s-Guide/tree/master/Ch3-Backup-and-Restore/Restore/restore-yamls.sh

If Vulnerability Advisor is not installed, ignore the errors.

4. Several files created during the initial cluster installation need to be reapplied:
   a. Change the directory to `<installation_directory>/cluster/cfc-components/`:

      `cd <installation_directory>/cluster/cfc-components/`

   b. Apply the `bootstrap-secret.yaml` file:

      `kubectl apply -f bootstrap-secret.yaml`

   c. Apply the `tiller.yaml` file:

      `kubectl apply -f tiller.yaml`

   d. Apply the `image-manager.yaml` file:

      `kubectl apply -f image-manager/image-manager.yaml`

   e. Apply the whole `storage` directory:

      `kubectl apply -f storage/`

5. Restore the resources that use IP addresses in the YAML configuration. Run the script in Example 3-17.

Example 3-17 The restore-ip-yamls.sh script

```
#!/bin/bash

# Set files
files=(
servicecatalog.yaml
daemonset.extensions/service-catalog-apiserver.yaml
daemonset.extensions/auth-idp.yaml
daemonset.extensions/calico-node.yaml
```