6.4.3 LimitRange

This admission controller will observe the incoming request and ensure that it does not violate any of the constraints enumerated in the LimitRange object in a namespace.

6.4.4 AlwaysPullImages

This admission controller modifies every new pod to force the image pull policy to Always. This is useful in a multitenant cluster so that users can be assured that their private images can be used only by those who have the credentials to pull them. Without this admission controller, once an image has been pulled to a node, any pod from any user can use it simply by knowing the image's name (assuming the pod is scheduled onto the right node), without any authorization check against the image. When this admission controller is enabled, images are always pulled prior to starting containers, which means valid credentials are required.

IBM Cloud Private supports all of the Kubernetes admission controllers. For more details see the following link:

https://kubernetes.io/docs/reference/access-authn-authz/admission-controllers/

6.5 Image security

IBM Cloud Private component Image Manager runs on top of the Docker registry V2 API. It integrates with the Docker registry to provide a local registry service, The Image Manager uses the cluster's authentication service to authenticate the end user. The Docker command line client is used to push or pull images in your cluster.

Figure 6-5 on page 249 shows the Image Manager architecture.