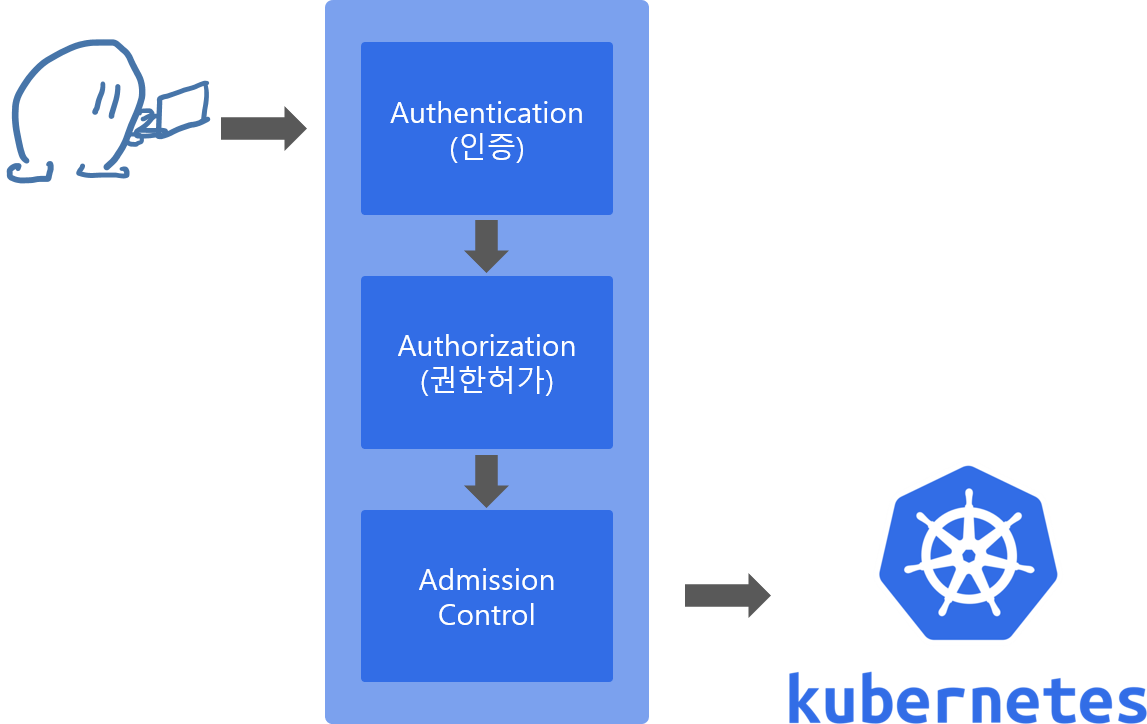
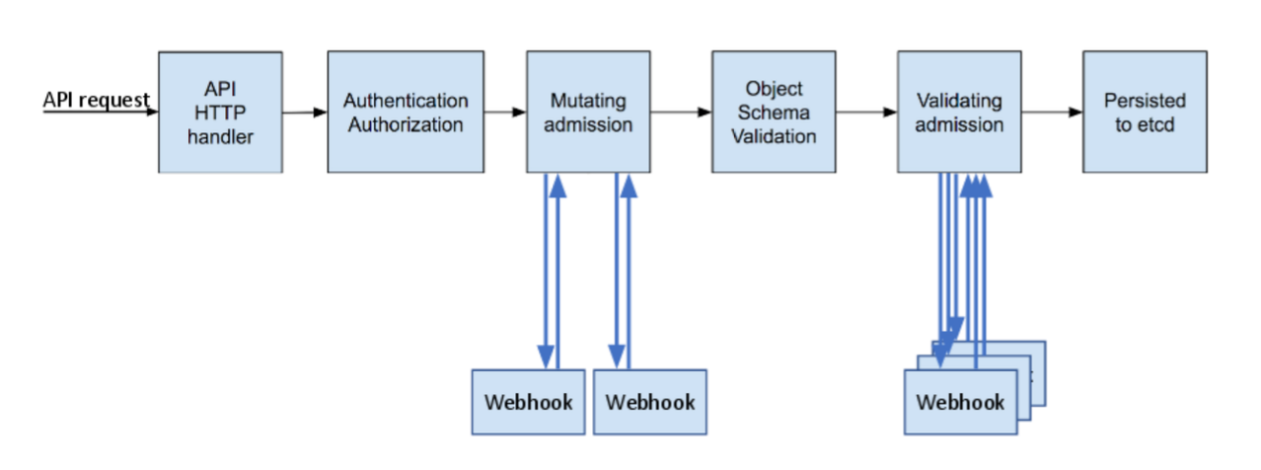
**Kubernetes의 Admission control이란?**

쿠버네티스의 접근제어는 크게 3단계가 있다.



* Authentication: 접속한 사람의 신분을 시스템이 인증하는 단계.
* Authorization: 누가 어떤 권한을 가지고 어떤 행동을 할 수 있는지 확인하는 단계.
* Admission Control: 인증과 권한확인 이후 추가적으로 요청 내용에 대한 검증이나 요청 내용을 강제로 변경할 때 사용한다.
* Authorization vs Admission control의 차이
  + Authorization 단계는 말그대로 사용자가 특정 작업을 수행할 때 어떤 권한이 있는지를 확인하는 단계이다. 반대로 Admission Control은 권한이 있는 사용자에 한해서 관리자가 추가로 특정 행동을 제한 혹은 변경하는 작업이다.

**Dynamic Admission Controller**



Admission Control도 Webhook으로 사용자에게 API가 열려있다. 쿠버네티스가 정의한 인터페이스만 잘 맞춘다면 사용자는 자신만의 Admission Controller를 구현할 수 있다. 쿠버네티스에서는 이것을 Dynamic Admission Controller라고 부르고 크게 MutatingWebhook과 ValidatingWebhook으로 나뉜다.

* MutatingWebhook: 사용자가 요청한 Request에 대해서 관리자가 임의로 값을 변경하는 작업이다. 예를들어, 사용자가 아무리 다른 ServiceAccount를 사용하더라도 무조건 default ServiceAccount를 사용하게끔 강제하는 경우 사용할 수 있다.
* ValidatingWebhook: 사용자가 요청한 Request에 대해서 관리자가 허용을 막는 작업이다.예를 들어, 사용자가 Default serviceaccount를 사용하지 않는 경우 에러메시지와 함께 요청을 반려하고 싶은 경우 사용할 수 있다.

**Kyverno란?**

kyverno는 새로운 k8s용 정책 엔진으로 정책을 k8s 자원으로 관리할 수 있게 해준다. 기존에 소개했었던 OPA와는 다르게 전용 정책 언어는 없으며 순수하게 CR만으로 정책을 표현하고 이에 따른 수행을 한다. 이에 따라 익숙한 도구인 kubectl, git, kustomize들을 직접 사용할 수 있다. Kyverno 정책을 사용하여 k8s의 자원들을 검증하고, 변경하고, 생성할 수 있다. 이를 사용해 CI/CD 파이프라인 등에 적용할 수 있다.

구조

