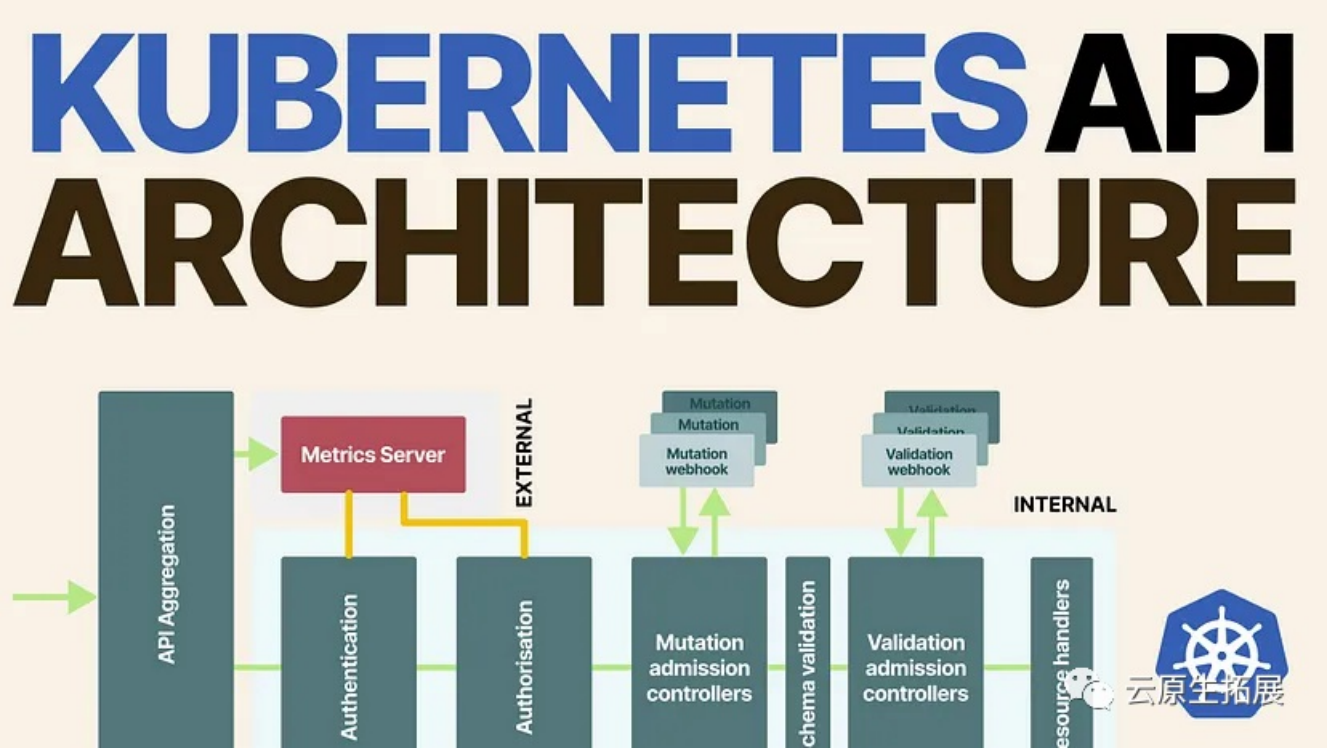
69Kubernetes 系列（六十三）Kubernetes API 架构

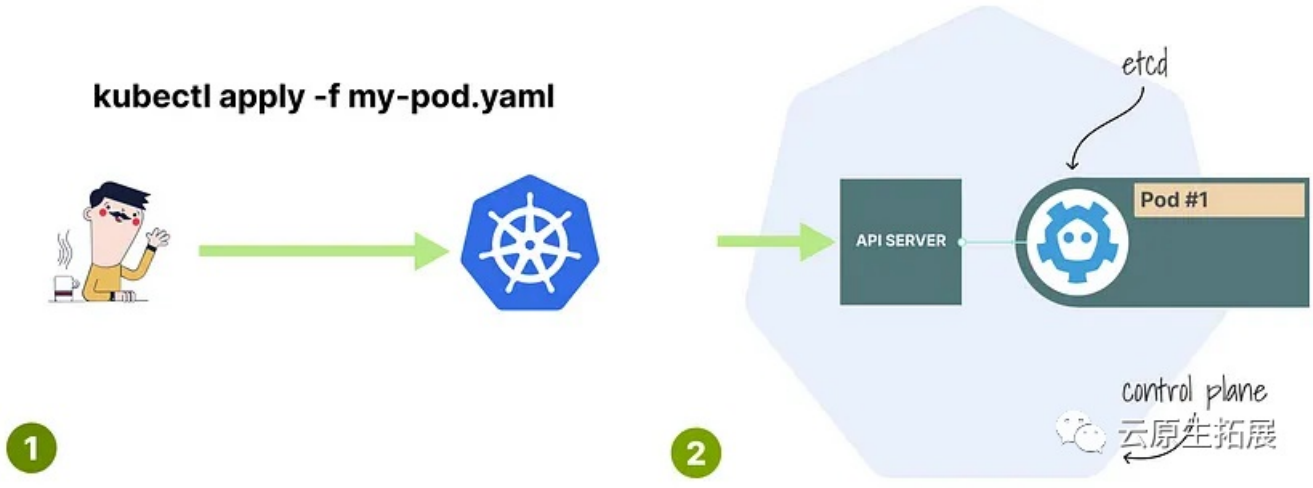
Kubernetes API Server 处理对 Kubernetes 集群的所有请求。

但它实际上是如何工作的呢？



当您键入 `kubectl apply -f my.yaml` 时，您的 YAML 将发送到 API 并存储在 etcd 中。

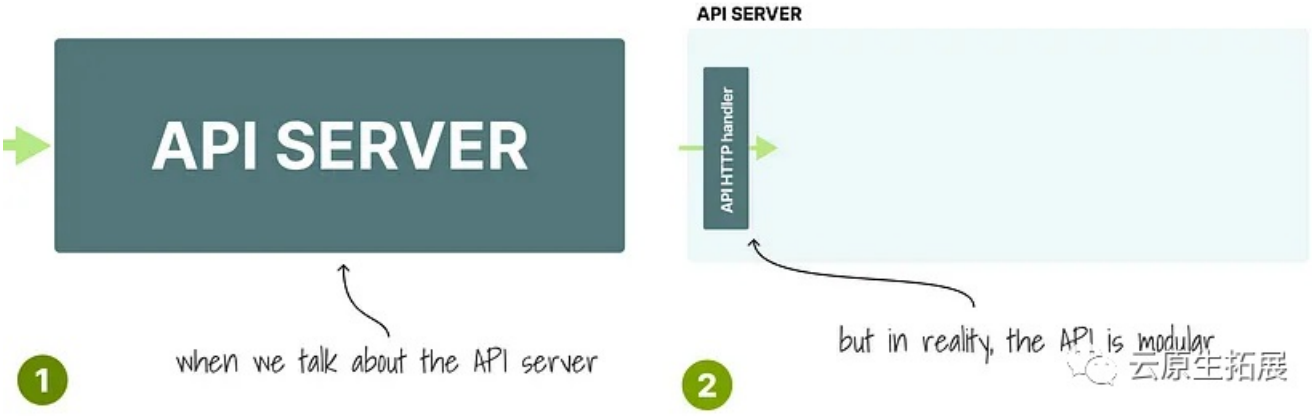
但是 API 服务器在做什么？



API 在图中只有一个块，但实际情况是有多个组件按顺序处理您的请求。

第一个模块是 HTTP 处理程序

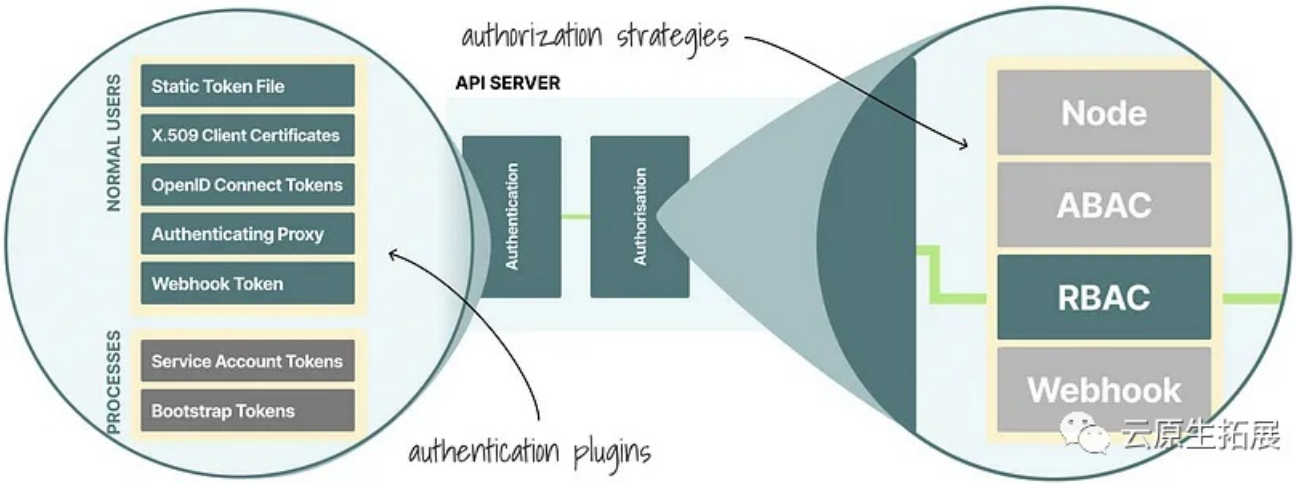
这只不过是一个普通的网络服务器。



API 收到请求后，必须确保：

- 您有权访问集群（身份验证）。
- 可以创建、删除、列出等资源（授权）。

这是(https://learnk8s.io/rbac-kubernetes)评估 RBAC 规则的部分。

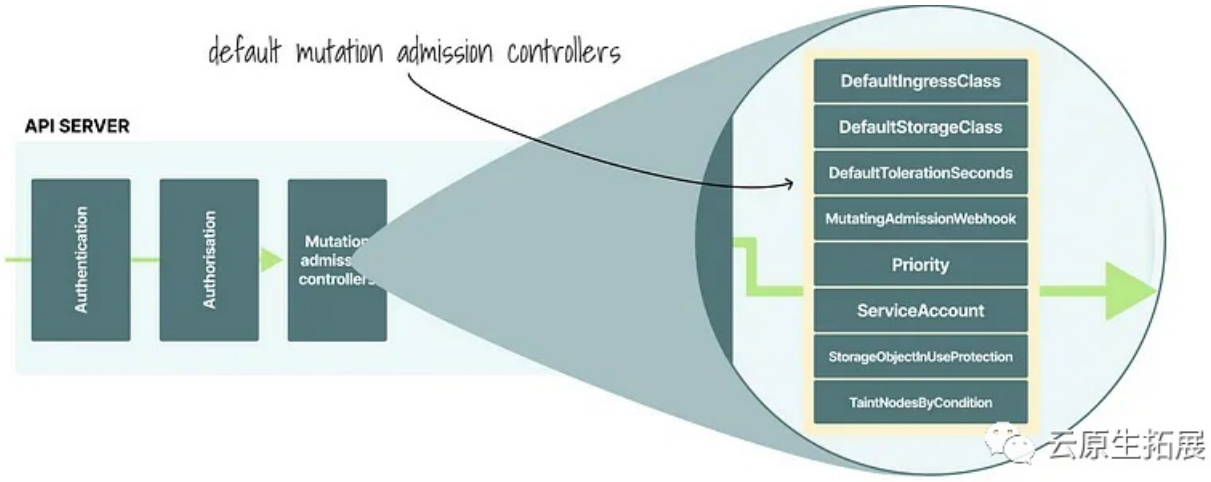


所以你通过了身份验证，你可以创建 Pod；下一步是什么？

API 将请求传递给 Mutation Admission Controller

Mutation Admission Controller (https://kubernetes.io/docs/reference/access-authn-authz/admission-controllers/) 负责查看您的 YAML 并对其进行修改.

不过，您可以用它更改什么 YAML？



您的 Pod 有镜像拉取策略吗？

如果没有，准入控制器将为您添加“Always”值。

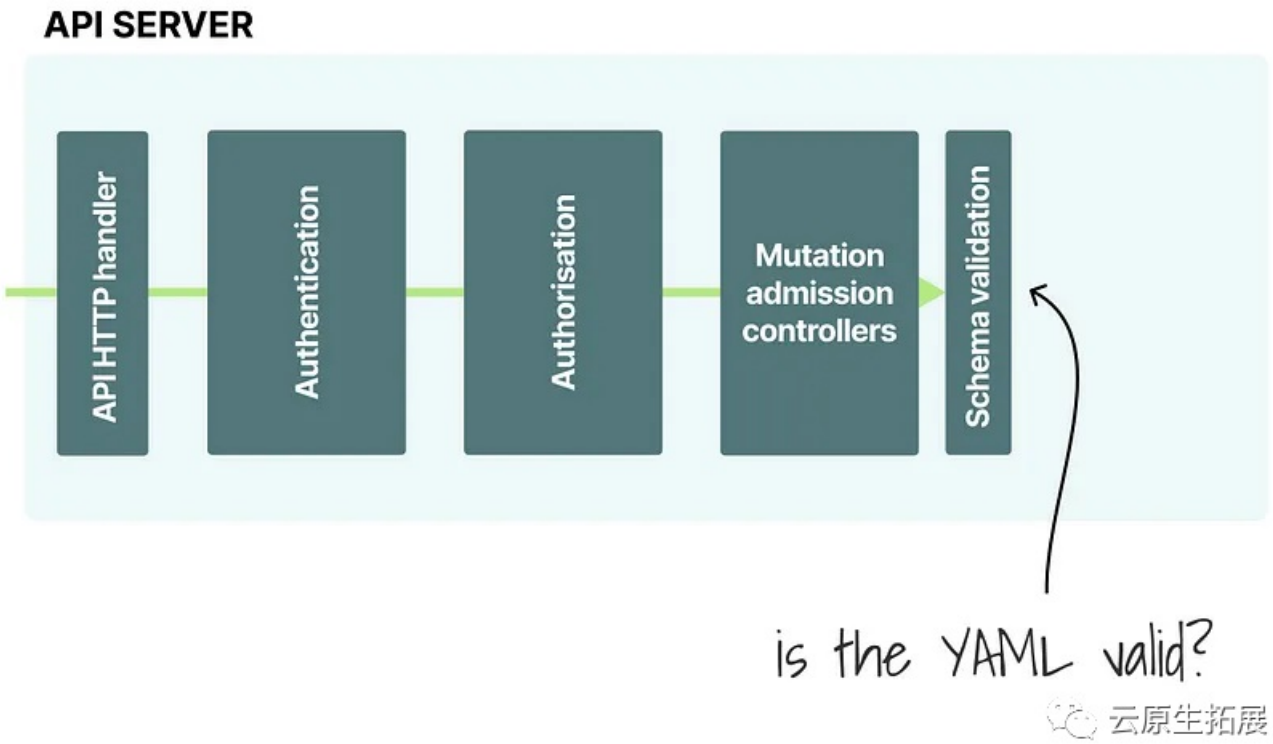
资源是 Pod 吗？

1. 它设置默认服务帐户（如果未设置）。
2. 添加带有 token 的卷。

还有更多！

经过所有修改，Pod 看起来还是 Pod 的样子吗？

API 进行快速检查以确保资源对内部架构有效。 您不希望集群中存储格式错误的 YAML。

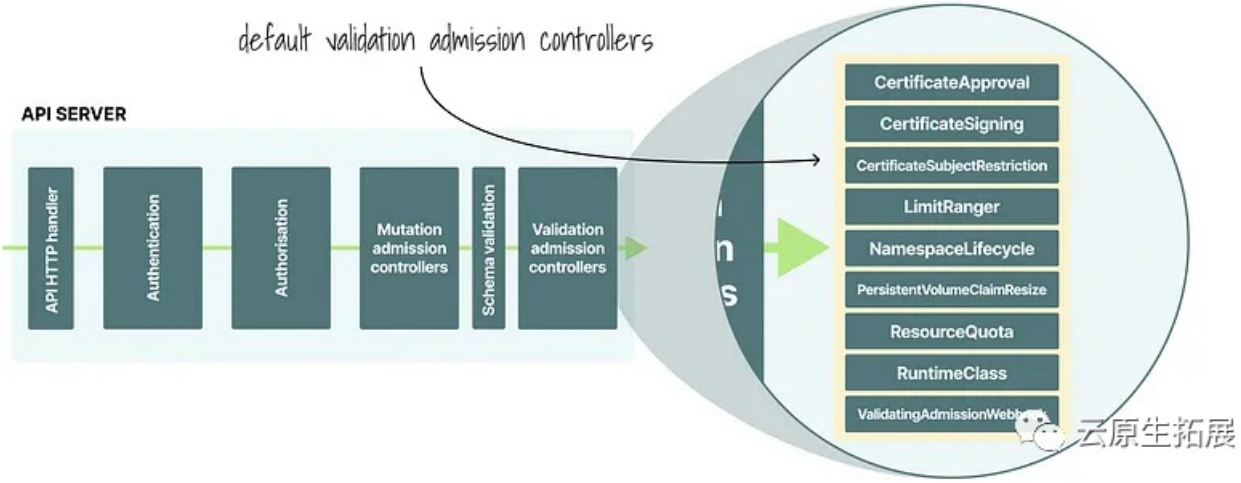


如果你试图在一个不存在的命名空间中部署一个 Pod，有人会阻止你吗？ 接下来说到：Validation Admission Controller(https://learnk8s.io/kubernetes-policies)

验证准入控制器

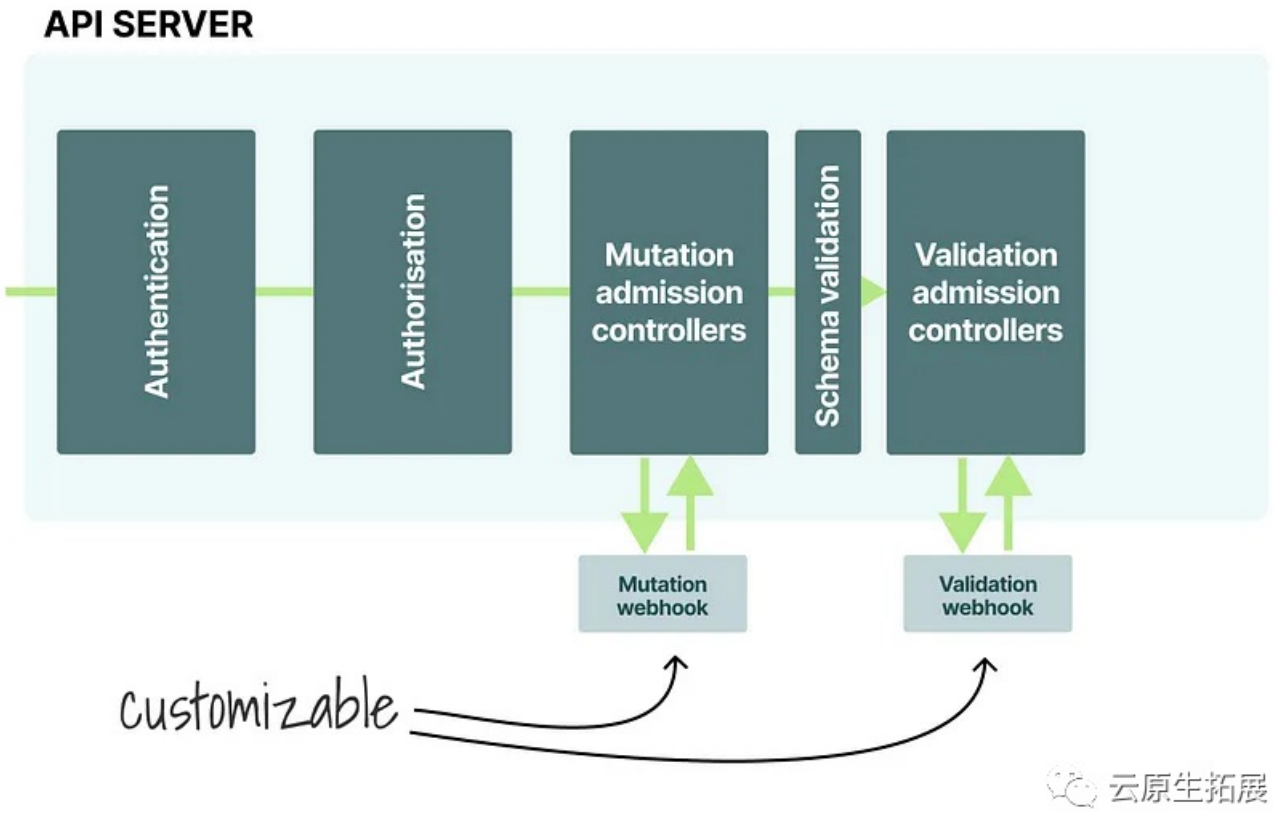
您是否尝试部署超过配额的资源？

控制器也会阻止这种情况。



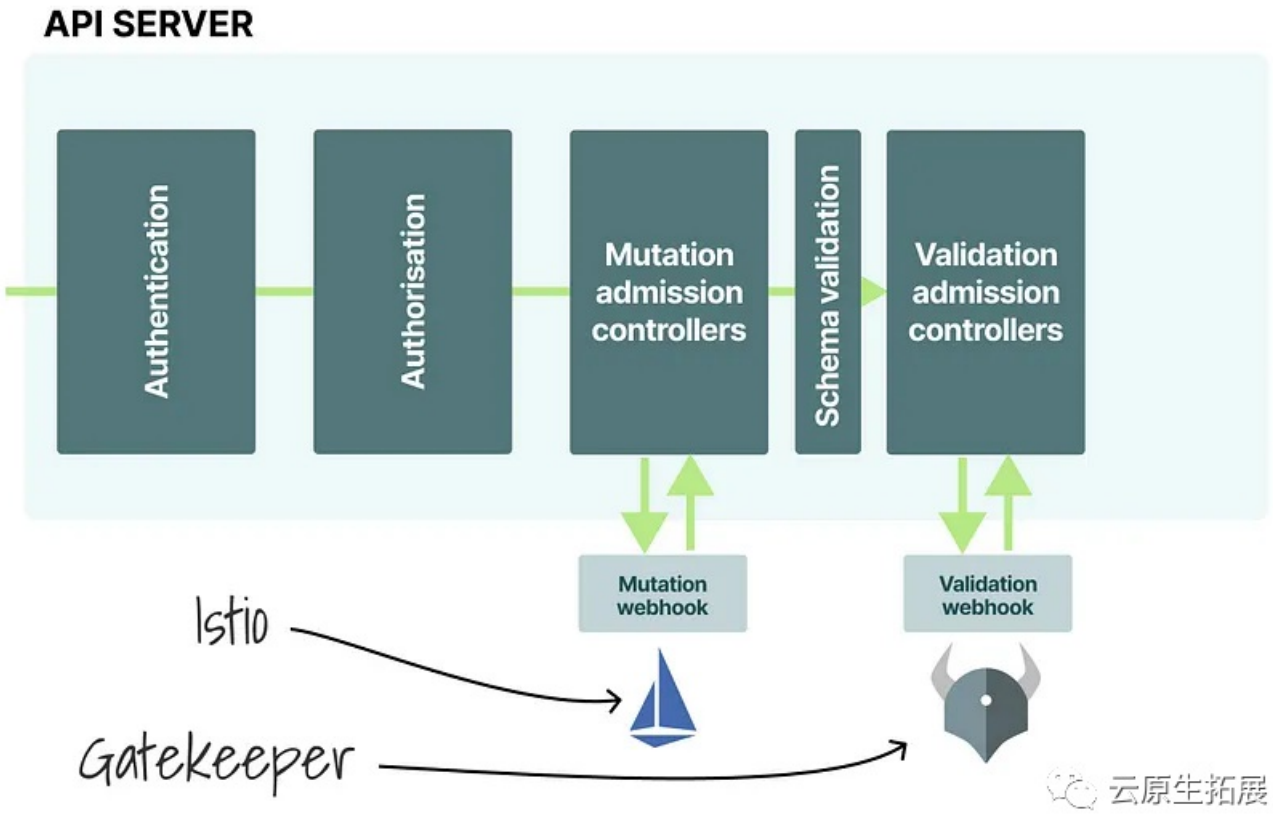
Validation 和 Mutation Admission 控制器也是可定制的。

您可以注册您的脚本并设计您的检查来决定是否应该拒绝资源到达 etcd。



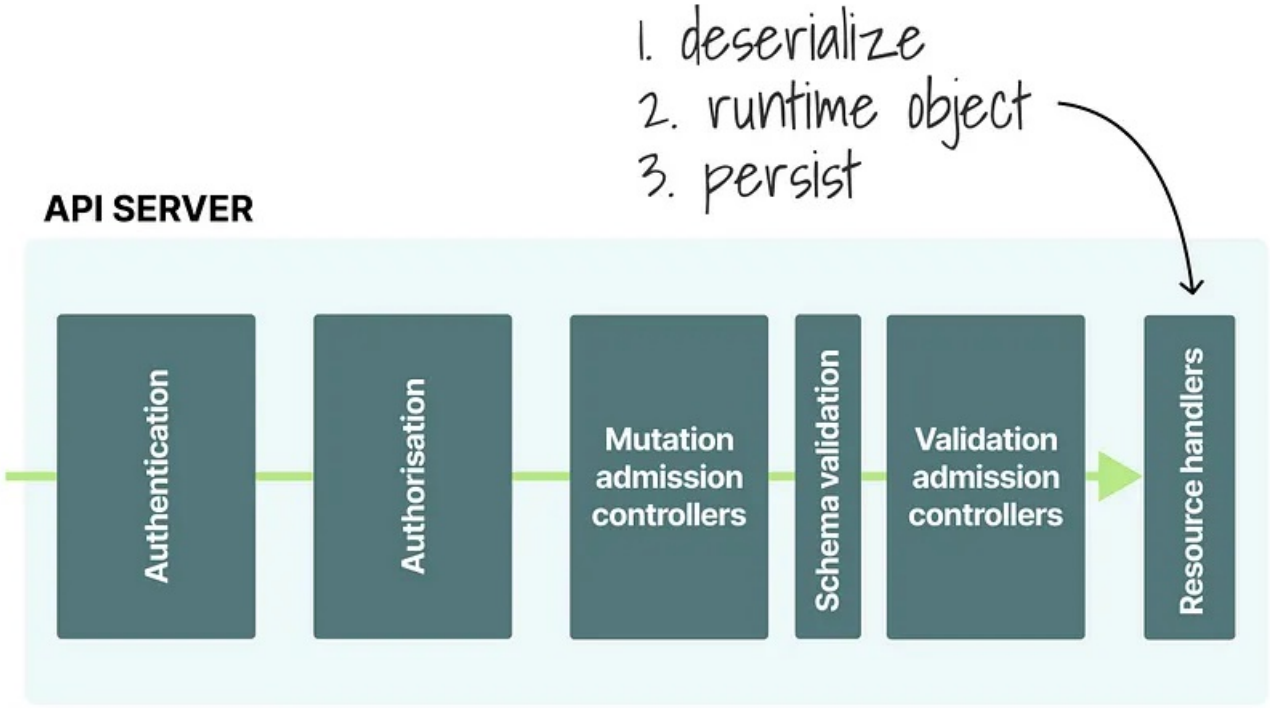
自定义 Admission 控制器的两个优秀示例：

- Istio 会自动向所有 Pod 注入一个额外的容器（mutation）。
- Gatekeeper（Open Policy Agent）根据策略检查您的资源并报告违规情况（validation）。



如果您设法通过了 Validation Admission Controller，您的资源将安全地存储在 etcd 中。

1. 请求被反序列化。
2. 在内存中创建运行时对象。
3. 最后，新的表示被持久化在 etcd 中。



值得注意的是，当您在 YAML 中定义 Pod 时，它们具有版本。

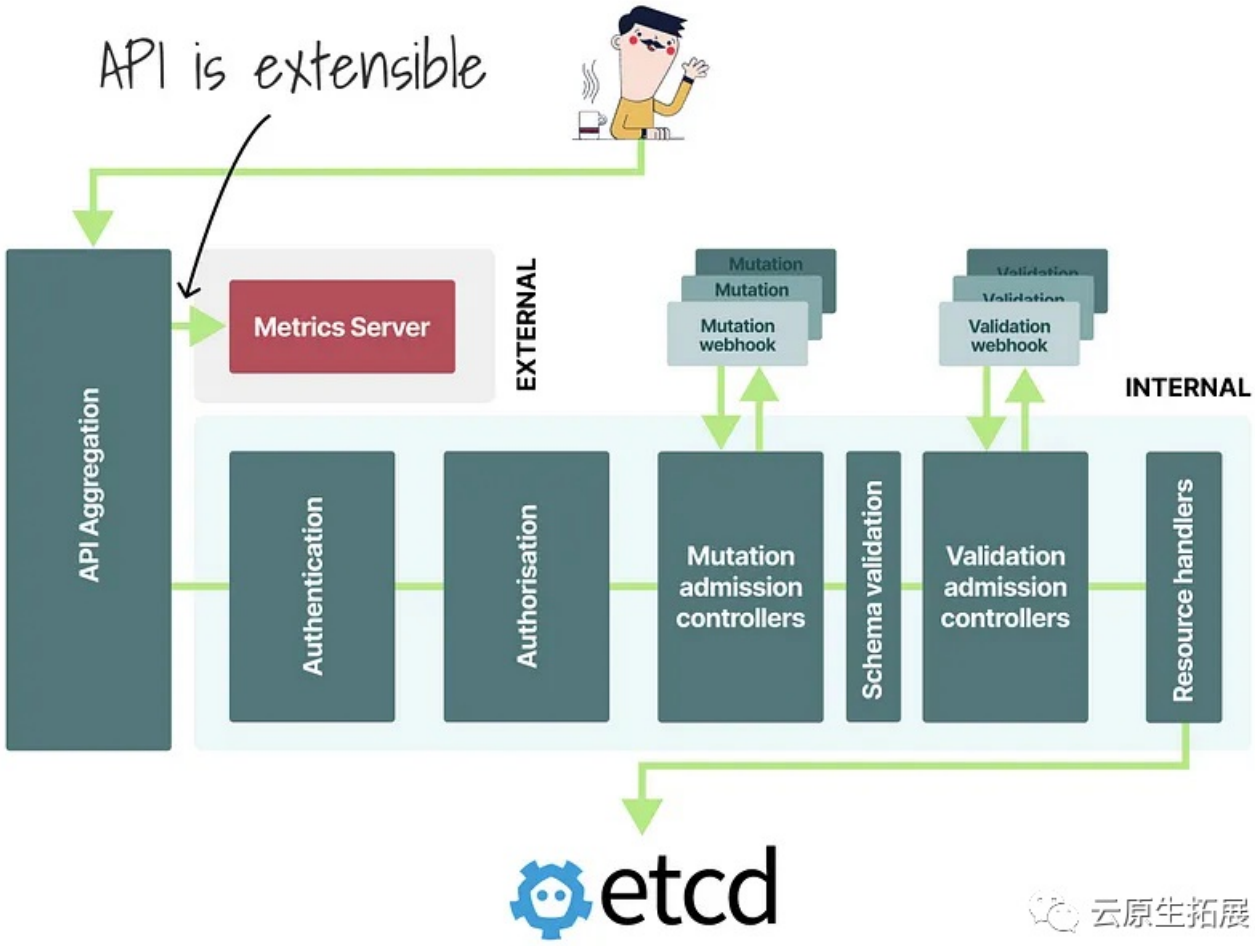
但是，同一个 Pod 存入数据库时是没有版本的。

它与内部表示一起存储，稍后可以将其反序列化为一个版本。

最后，Kubernetes API 也是可扩展的！

您可以添加自己的 API 并将它们注册到 Kubernetes。

一个很好的例子是 metrics API 服务。



metrics API server 将自己注册到 API 并公开额外的 API 端点。

值得注意的是，您可以与 API 的其余部分集成，并使用 API Server 中现有的身份验证和授权模块。