# Sentinel的概念和功能

## 基本概念

### 资源

**资源就是Sentinel要保护的东西**

资源是 Sentinel 的关键概念。它可以是 Java 应用程序中的任何内容，可以是一个服务，也可以是一个方法，甚至可以是一段代码。

我们入门案例中的message1方法就可以认为是一个资源

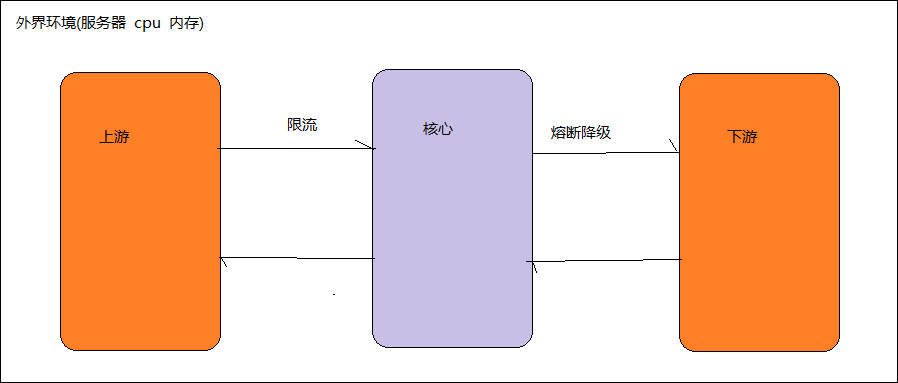
### 规则

**规则就是用来定义如何进行保护资源的**

作用在资源之上, 定义以什么样的方式保护资源，主要包括流量控制规则、熔断降级规则以及系统保护规则。

我们入门案例中就是为message1资源设置了一种流控规则, 限制了进入message1的流量

## 重要功能



Sentinel的主要功能就是容错，主要体现为下面这三个：

### 流量控制

流量控制在网络传输中是一个常用的概念，它用于调整网络包的数据。任意时间到来的请求往往是 随机不可控的，而系统的处理能力是有限的。我们需要根据系统的处理能力对流量进行控制。Sentinel 作为一个调配器，可以根据需要把随机的请求调整成合适的形状。

### 熔断降级

当检测到调用链路中某个资源出现不稳定的表现，例如请求响应时间长或异常比例升高的时候，则 对这个资源的调用进行限制，让请求快速失败，避免影响到其它的资源而导致级联故障。

Sentinel 对这个问题采取了两种手段: 通过并发线程数进行限制

Sentinel 通过限制资源并发线程的数量，来减少不稳定资源对其它资源的影响。当某个资源出现不稳定的情况下，例如响应时间变长，对资源的直接影响就是会造成线程数的逐步堆 积。当线程数在特定资源上堆积到一定的数量之后，对该资源的新请求就会被拒绝。堆积的 线程完成任务后才开始继续接收请求。

通过响应时间对资源进行降级

除了对并发线程数进行控制以外，Sentinel 还可以通过响应时间来快速降级不稳定的资源。当依赖的资源出现响应时间过长后，所有对该资源的访问都会被直接拒绝，直到过了指定的 时间窗口之后才重新恢复。

**Sentinel 和 Hystrix 的区别**

两者的原则是一致的, 都是当一个资源出现问题时, 让其快速失败, 不要波及到其它服务但是在限制的手段上, 确采取了完全不一样的方法:

Hystrix 采用的是线程池隔离的方式, 优点是做到了资源之间的隔离, 缺点是增加了线程切换的成本。

Sentinel 采用的是通过并发线程的数量和响应时间来对资源做限制。

### 系统负载保护

Sentinel 同时提供系统维度的自适应保护能力。当系统负载较高的时候，如果还持续让请求进入可能会导致系统崩溃，无法响应。在集群环境下，会把本应这台机器承载的流量转发到其 它的机器上去。如果这个时候其它的机器也处在一个边缘状态的时候，Sentinel 提供了对应的保护机制，让系统的入口流量和系统的负载达到一个平衡，保证系统在能力范围之内处理最多的请 求。

**总之一句话: 我们需要做的事情，就是在Sentinel的资源上配置各种各样的规则，来实现各种容错的功能。**

每秒请求量大于3的时候开始限流。