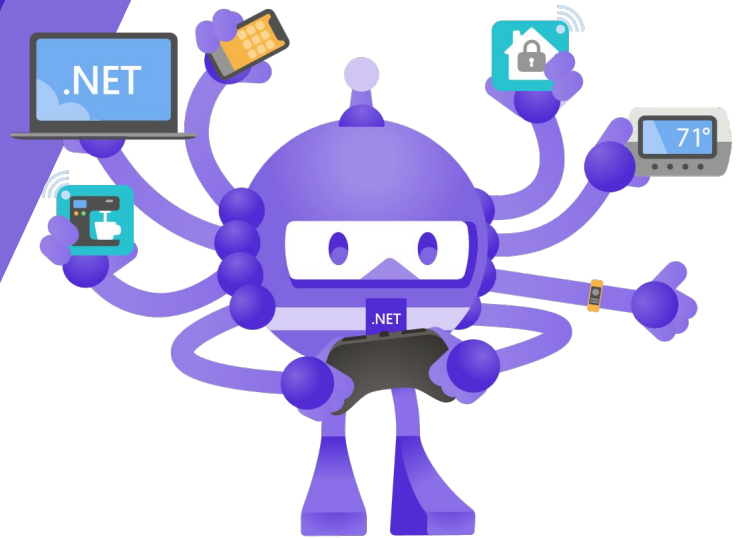
.NET Conference 2023

Proteggiamo le nostre API con il rate limiting



Microsoft avanade

altitudo BC Soft consulenza sistemi informativi Packt

UNIKEY Bringing IT knowledge to the people Reti Società Benefit stickermule JET BRAINS

SPONSOR


Microsoft


avanade


altitudo


BC Soft
consulenza sistemi informativi


Reti
Società Benefit


UNIKEY
Bringing IT knowledge to the people


JET
BRAINS


Packt


NET
CODE

Di cosa parleremo?

La nostra applicazione sta avendo successo

Da X anni siamo leader del nostro settore.
Abbiamo quindi deciso di...

Di cosa parleremo?

...APRIRCI ai DEVELOPERS!
Da un'analisi di mercato, le integrazioni...

La nostra applicazione sta avendo successo
Da X anni siamo leader del nostro settore.
Abbiamo quindi deciso di...

Di cosa parleremo?

...APRIRCI ai DEVELOPERS!
Da un'analisi di mercato, le integrazioni...

La nostra applicazione sta avendo successo
Da X anni siamo leader del nostro settore.
Abbiamo quindi deciso di...

Ci servono delle API!!!
E naturalmente questa è l'occasione per migrare il monolite a microservizi

Di cosa parleremo?

...APRIRCI ai DEVELOPERS!
Da un'analisi di mercato, le integrazioni...

La scelta di aprirci all'*infinito* ed inesplorato mondo delle integrazioni...
Celebrate!!!

La nostra applicazione sta avendo successo
Da X anni siamo leader del nostro settore.
Abbiamo quindi deciso di...

Ci servono delle API!!!
E naturalmente questa è l'occasione per migrare il monolite a microservizi

Di cosa parleremo?

...APRIRCI ai DEVELOPERS!
Da un'analisi di mercato, le integrazioni...

La scelta di aprirci all'*infinito* ed inesplorato mondo delle integrazioni...
Celebrate!!!

La nostra applicazione sta avendo successo
Da X anni siamo leader del nostro settore.
Abbiamo quindi deciso di...

Ci servono delle API!!!
E naturalmente questa è l'occasione per migrare il monolite a microservizi

In numero delle integrazioni cresce esponenzialmente!
1 ... 2 ... 4 ... 8 ... **9**

Di cosa parleremo?

...APRIRCI ai DEVELOPERS!
Da un'analisi di mercato, le integrazioni...

La scelta di aprirci all'*infinito* ed inesplorato mondo delle integrazioni...
Celebrate!!!

Non abbiamo abbastanza risorse!
Dobbiamo passare al cloud, così scala!

La nostra applicazione sta avendo successo
Da X anni siamo leader del nostro settore.
Abbiamo quindi deciso di...

Ci servono delle API!!!
E naturalmente questa è l'occasione per migrare il monolite a microservizi

In numero delle integrazioni cresce esponenzialmente!

1 ... 2 ... 4 ... 8 ... **9**

Di cosa parleremo?

...APRIRCI ai DEVELOPERS!
Da un'analisi di mercato, le integrazioni...

La scelta di aprirci all'*infinito* ed inesplorato mondo delle integrazioni...
Celebrate!!!

Non abbiamo abbastanza risorse!
Dobbiamo passare al cloud, così scala!

La nostra applicazione sta avendo successo
Da X anni siamo leader del nostro settore.
Abbiamo quindi deciso di...

Ci servono delle API!!!
E naturalmente questa è l'occasione per migrare il monolite a microservizi

In numero delle integrazioni cresce esponenzialmente!
1 ... 2 ... 4 ... 8 ... **9**

Il cloud ha scalato troppo

Cosa è successo qui?

...APRIRCI ai DEVELOPERS!
Da un'analisi di mercato, le integrazioni...

La scelta di aprirci all'*infinito* ed inesplorato mondo delle integrazioni...
Celebrate!!!

Non abbiamo abbastanza risorse!
Dobbiamo passare al cloud, così scala!

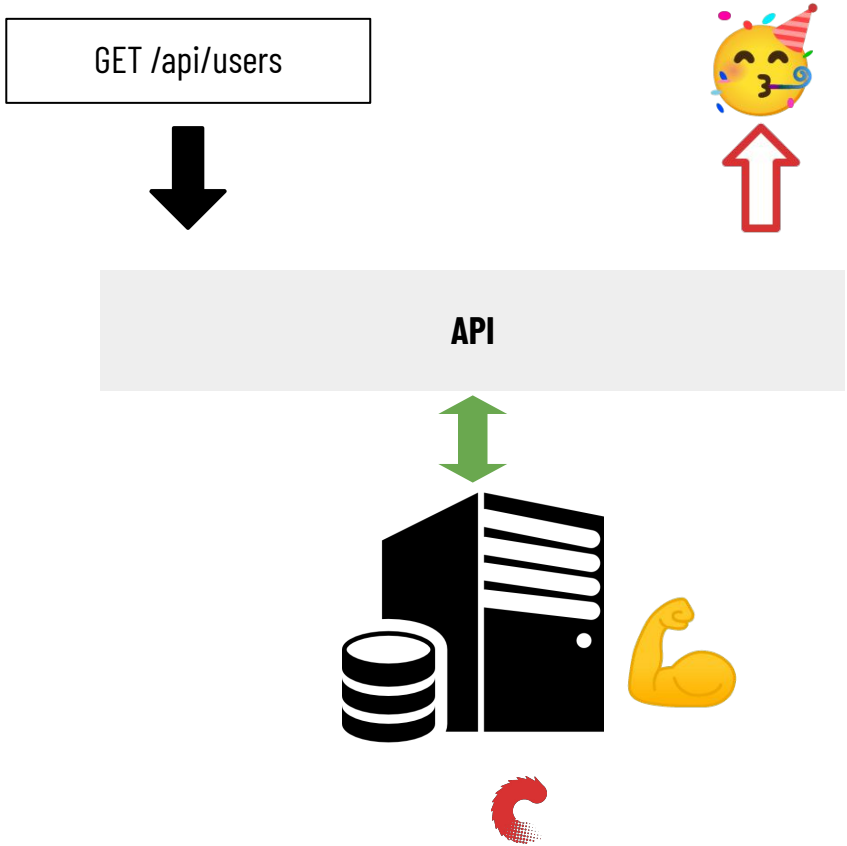
La nostra applicazione sta avendo successo
Da X anni siamo leader del nostro settore.
Abbiamo quindi deciso di...

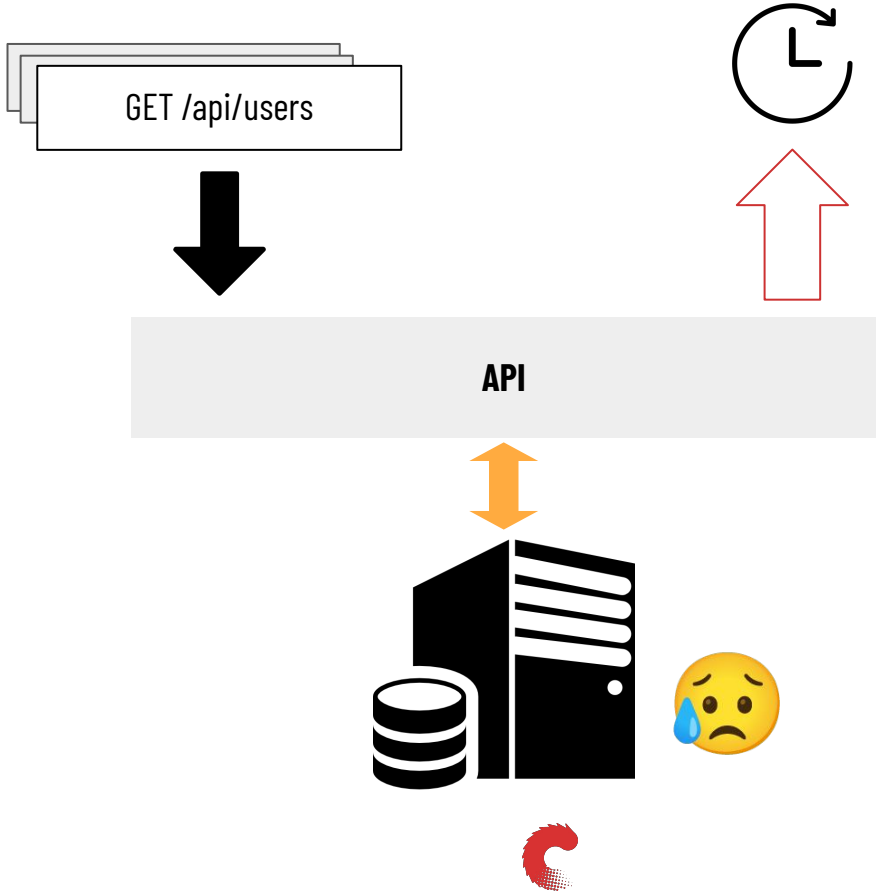
Ci servono delle API!!!
E naturalmente questa è l'occasione per migrare il monolite a microservizi

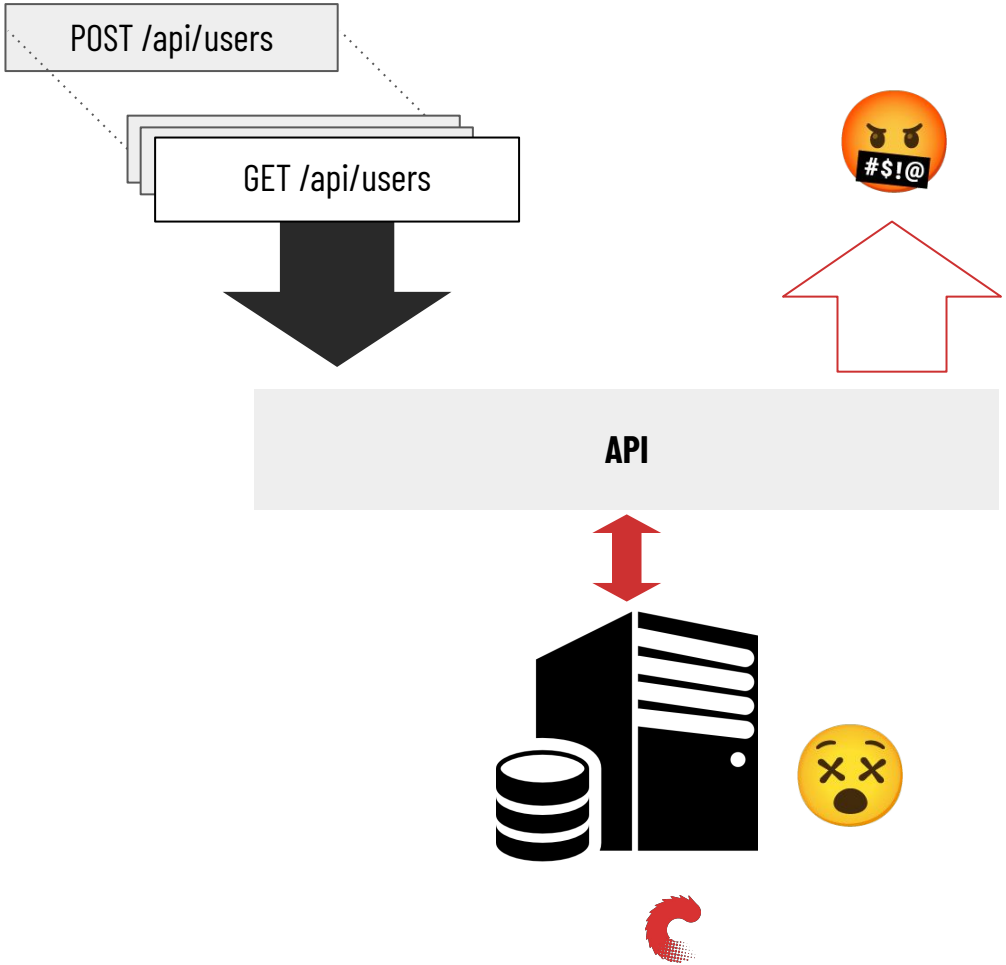
In numero delle integrazioni cresce esponenzialmente!

1 ... 2 ... 4 .. 8 ... **9**

Il cloud ha scalato troppo


GET /api/users
API


GET /api/users
API


POST /api/users
GET /api/users
#$!@
API

Services can only serve a limited number of requests per second.

If each user can make as many calls to the API as they like, the overload of requests can starve the servers and affect the response times for other consumers.

System Design Interview: API Rate Limiter


+750.000 logins alle 9:00 💪
RESTIAMO NELLA SFERA DELLA LEGALITÀ...

RESTIAMO NELLA SFERA DELLA LEGALITÀ...

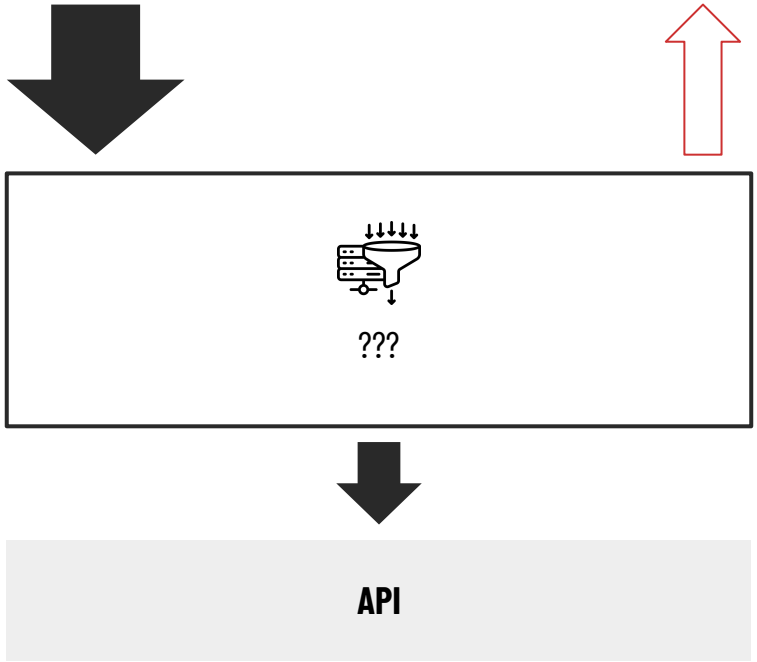
SPOSTIAMOCI NELLA SFERA DELLA MAGIA... 🪄


Denial of Service Attack
MENTRE NELLA SFERA DELL'ILLEGALITA'

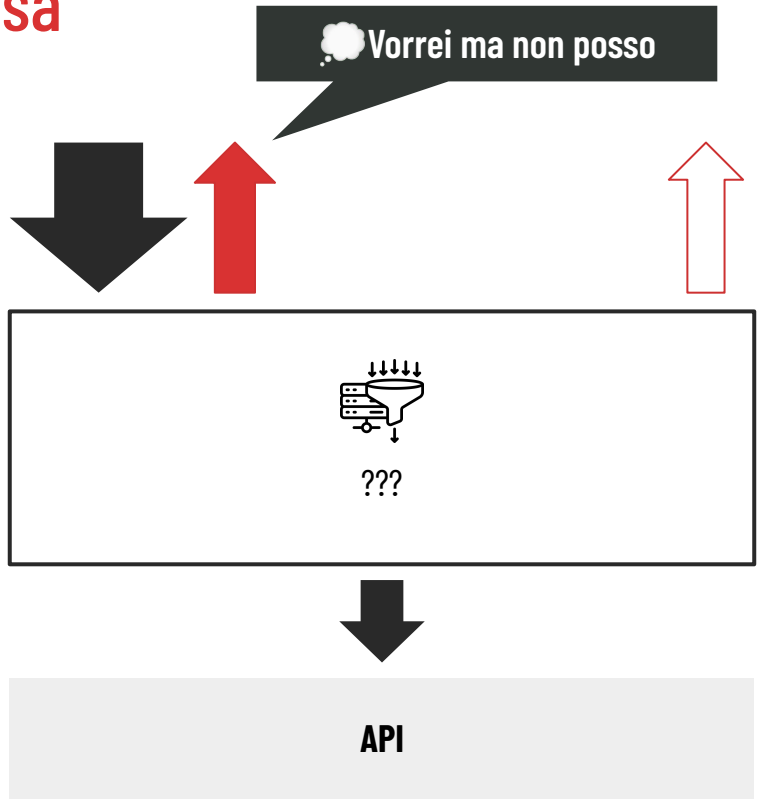

Denial of Service Attack
Malicious API attacks rose 681% in 2021 even with security measures in place and are predicted to become the primary attack vector in 2022
Achieve Internet
MENTRE NELLA SFERA DELL'ILLEGALITA'

Che cosa ci serve?

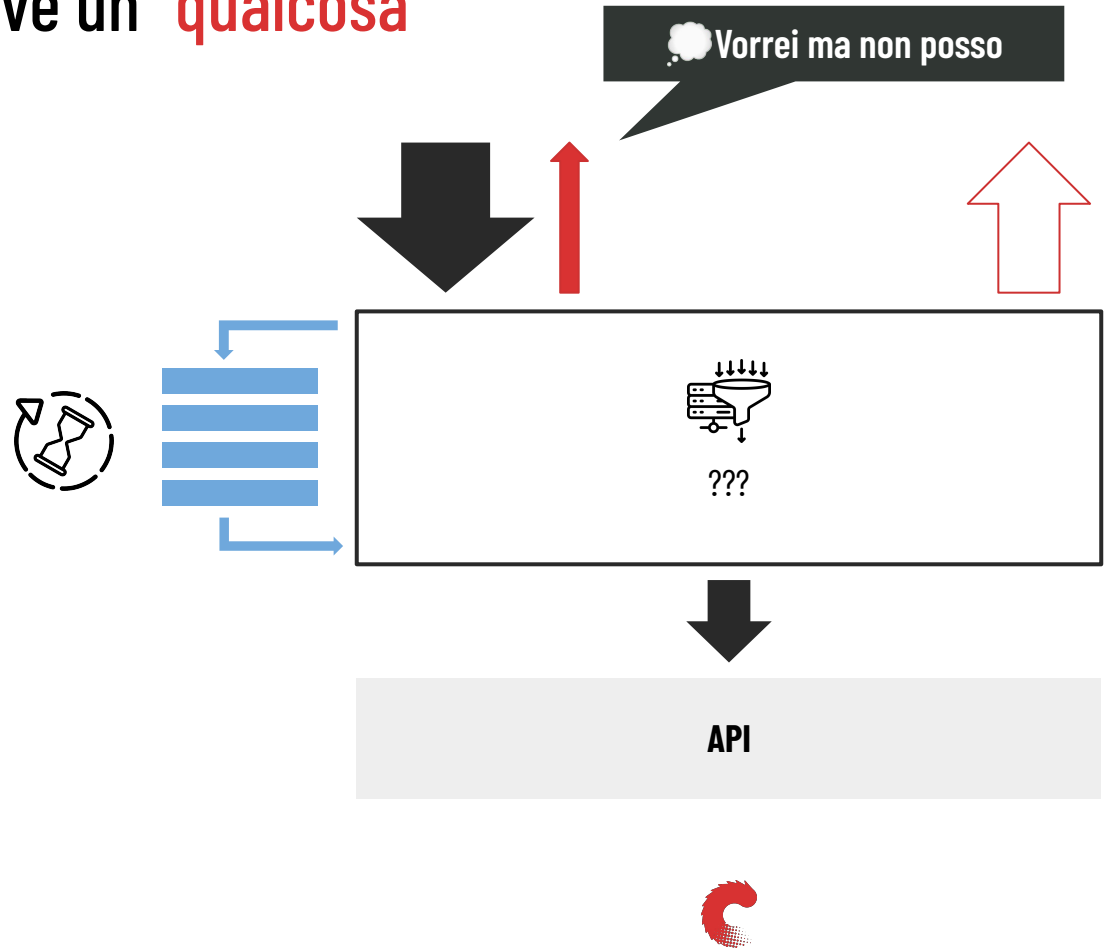
Ci serve un “qualcosa”



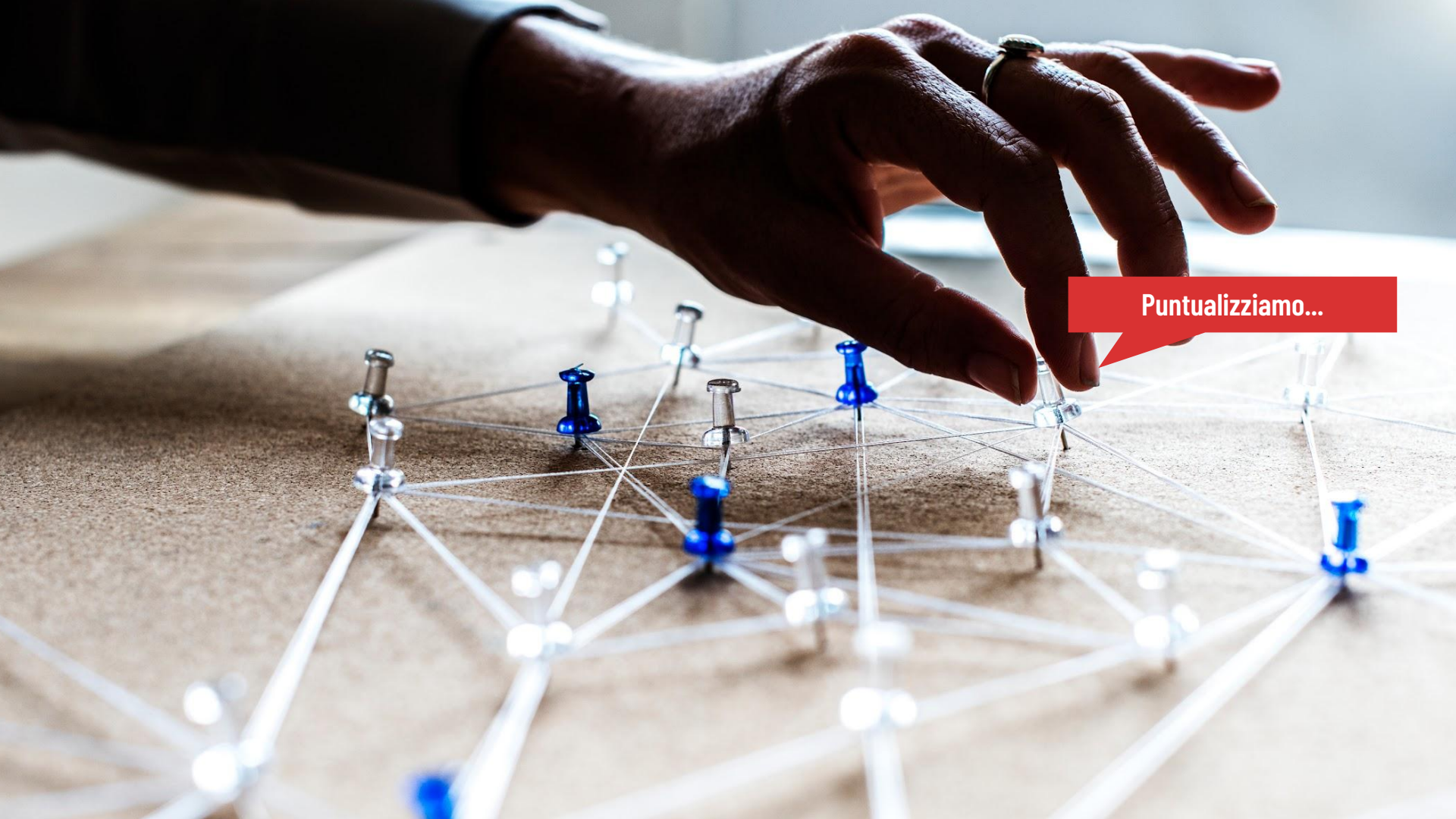
Ci serve un “qualcosa”



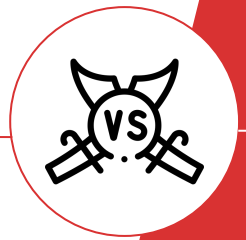
Ci serve un “qualcosa”



Ci serve un Rate Limiter!

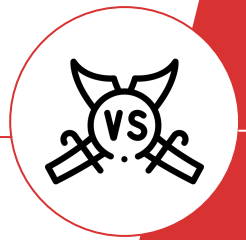

Puntualizziamo...

Throttling



Rate Limiting

Throttling



Rate Limiting

E' una tecnica per controllare il **numero di chiamate** (traffico) che una API può gestire. Utile per prevenire il **sovraccarico** dell'infrastruttura di rete e dei server

👍 **VANTAGGI:** Semplicità

👎 **SVANTAGGI**

- Puoi controllare il numero di richieste, ma non la quantità di dati scambiati
- I limiti si applicano a TUTTI gli utenti

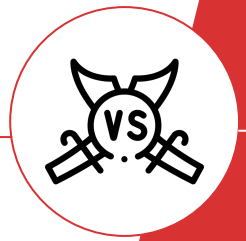
Throttling

E' una tecnica per controllare il **numero di chiamate** (traffico) che una API può gestire.
Utile per prevenire il **sovraccarico** dell'infrastruttura di rete e dei server

👍 **VANTAGGI:** Semplicità

👎 **SVANTAGGI**

- Puoi controllare il numero di richieste, ma non la quantità di dati scambiati
- I limiti si applicano a TUTTI gli utenti



Rate Limiting

E' una tecnica per controllare il **numero di richieste** che un utente/client può fare in un periodo di tempo

Utile per prevenire **l'abuso o l'utilizzo errato** di un'API

👍 **VANTAGGI**

- Evitare che l'utilizzo errato di un'API da parte di un utente abbia impatto sugli altri utenti
- Garantisce il rispetto dello SLA

👎 **SVANTAGGI**

Configurazione complessa

Throttling

E' una tecnica per controllare il **numero di chiamate** (traffico) che una API può gestire. Utile per prevenire il **sovraccarico** dell'infrastruttura di rete e dei server

👍 **VANTAGGI:** Semplicità

👎 **SVANTAGGI**

- Puoi controllare il numero di richieste, ma non la quantità di dati scambiati
- I limiti si applicano a TUTTI gli utenti

Rate Limiting

E' una tecnica per controllare il **numero di richieste** che un utente/client può fare in un periodo di tempo

Utile per prevenire **l'abuso o l'utilizzo errato** di un'API

👍 **VANTAGGI**

- Evitare che l'utilizzo errato di un'API da parte di un utente abbia impatto sugli altri utenti
- Garantisce il rispetto dello SLA

👎 **SVANTAGGI**

Configurazione complessa

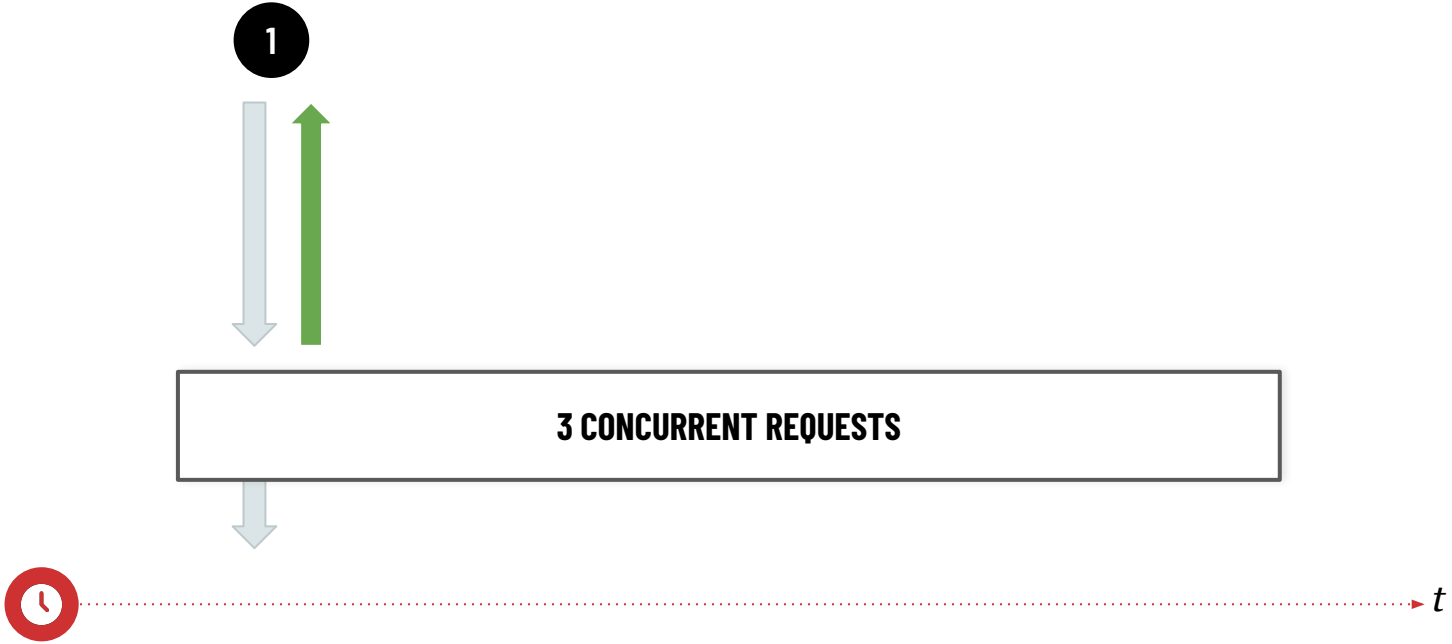
Tipologie di Rate Limiter

Concurrent Limit	Time Window Limit	Sliding Window Limit	Token Bucket Limit

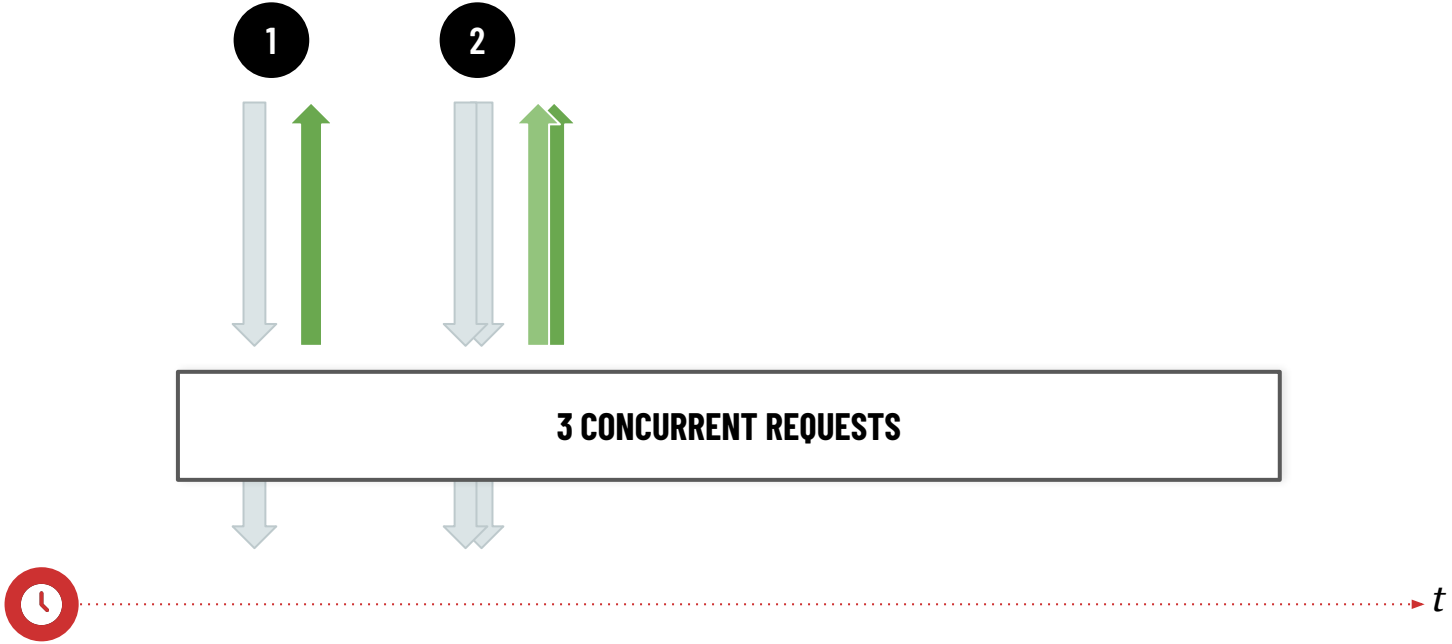
Tipologie di Rate Limiter

Concurrent Limit | Time Window Limit | Sliding Window Limit | Token Bucket Limit

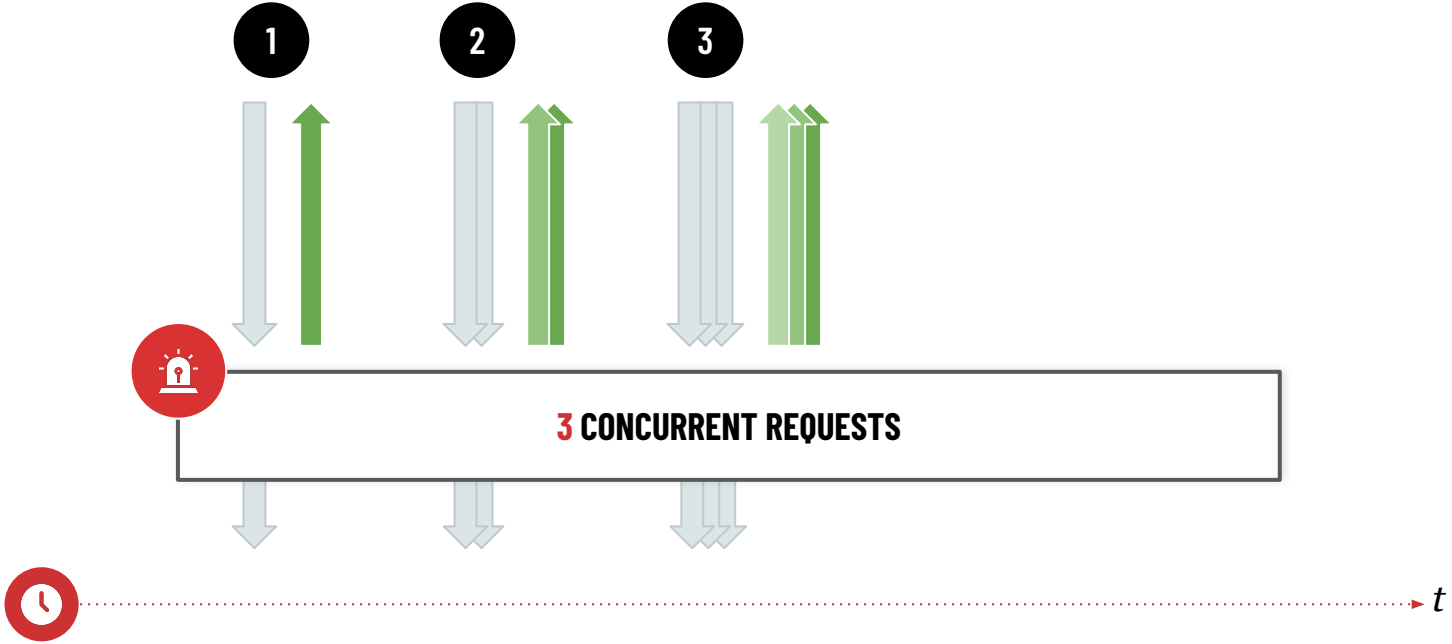
Tipologie di Rate limiting - Concurrent limit



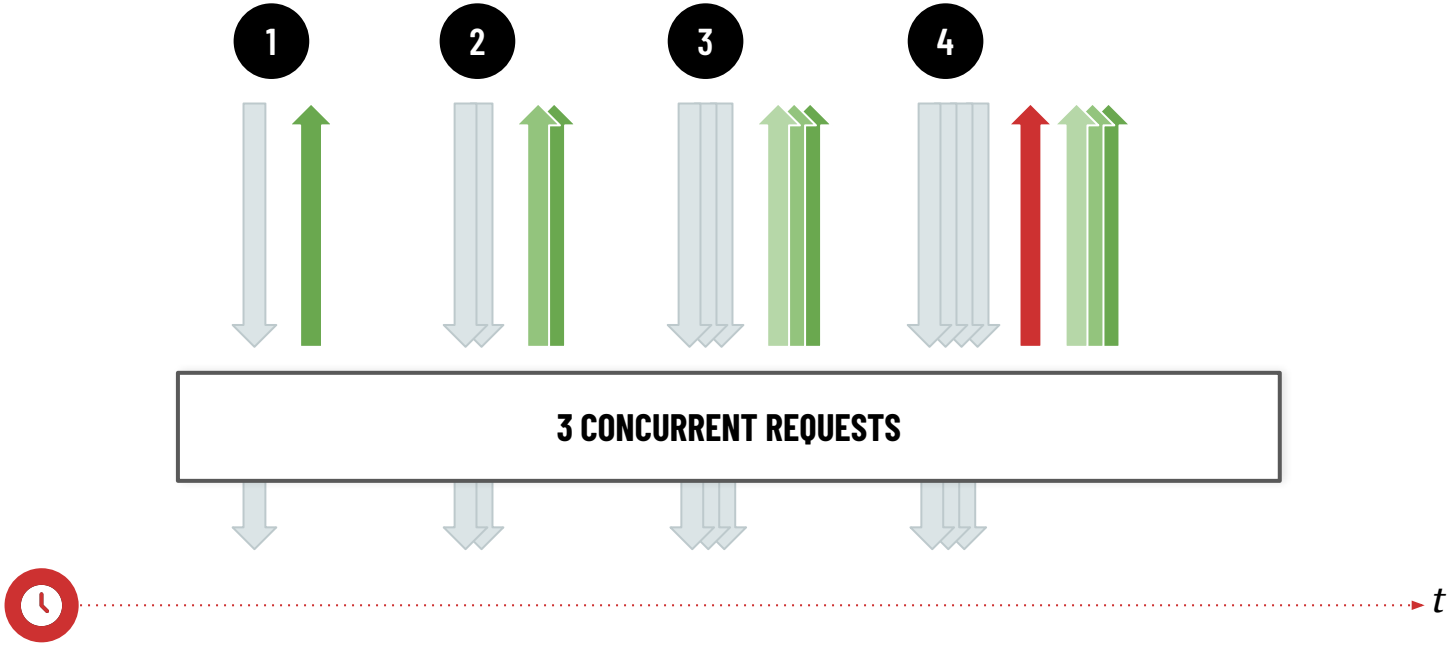
Tipologie di Rate limiting - Concurrent limit



Tipologie di Rate limiting - Concurrent limit



Tipologie di Rate limiting - Concurrent limit



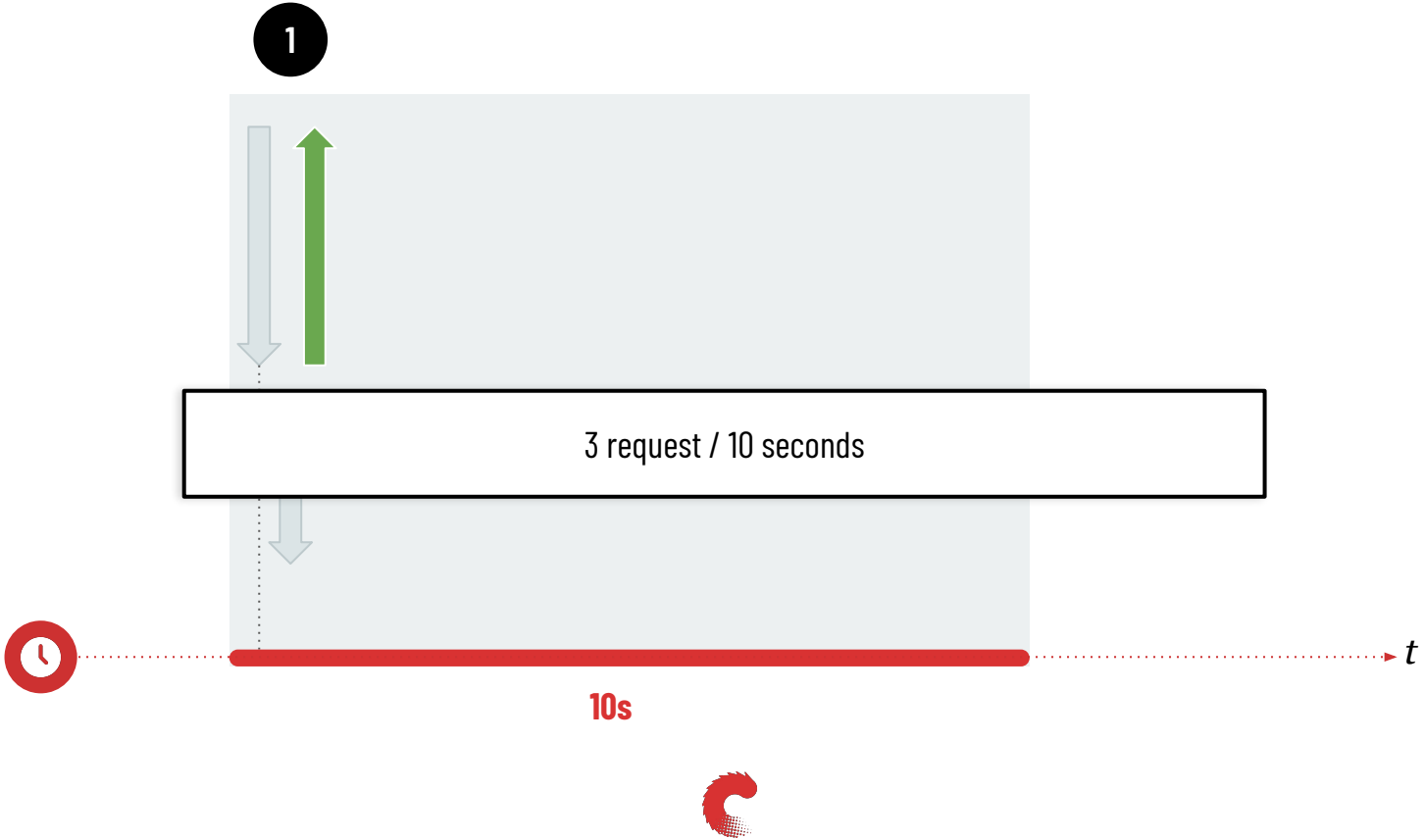
Tipologie di Rate limiting - Concurrent limit

- Con consente di tenere sotto controllo le risorse per endpoint CPU-intensive
- Ci aiuta mitigare i problemi dovuti ad attacchi DoS

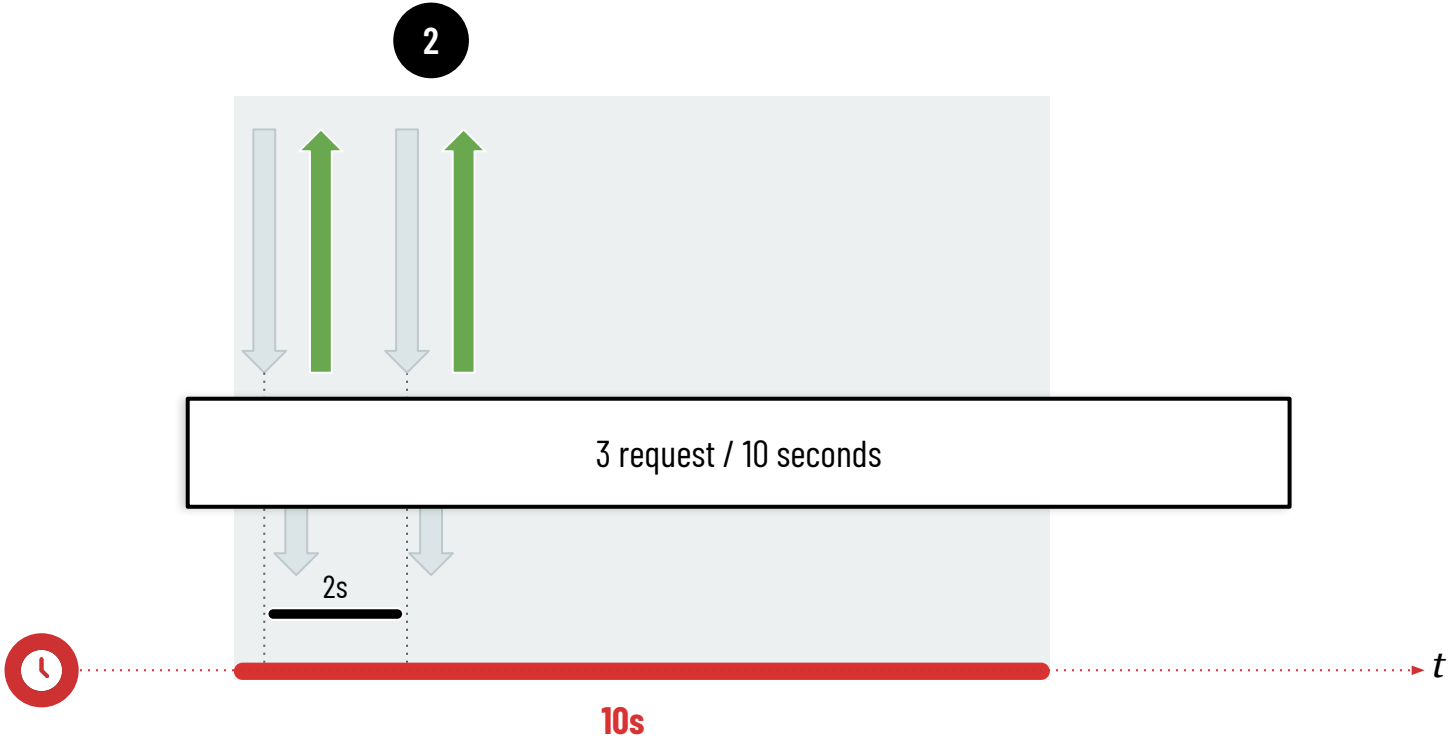
Tipologie di Rate Limiter

Concurrent Limit	**Time Window Limit**	Sliding Window Limit	Token Bucket Limit

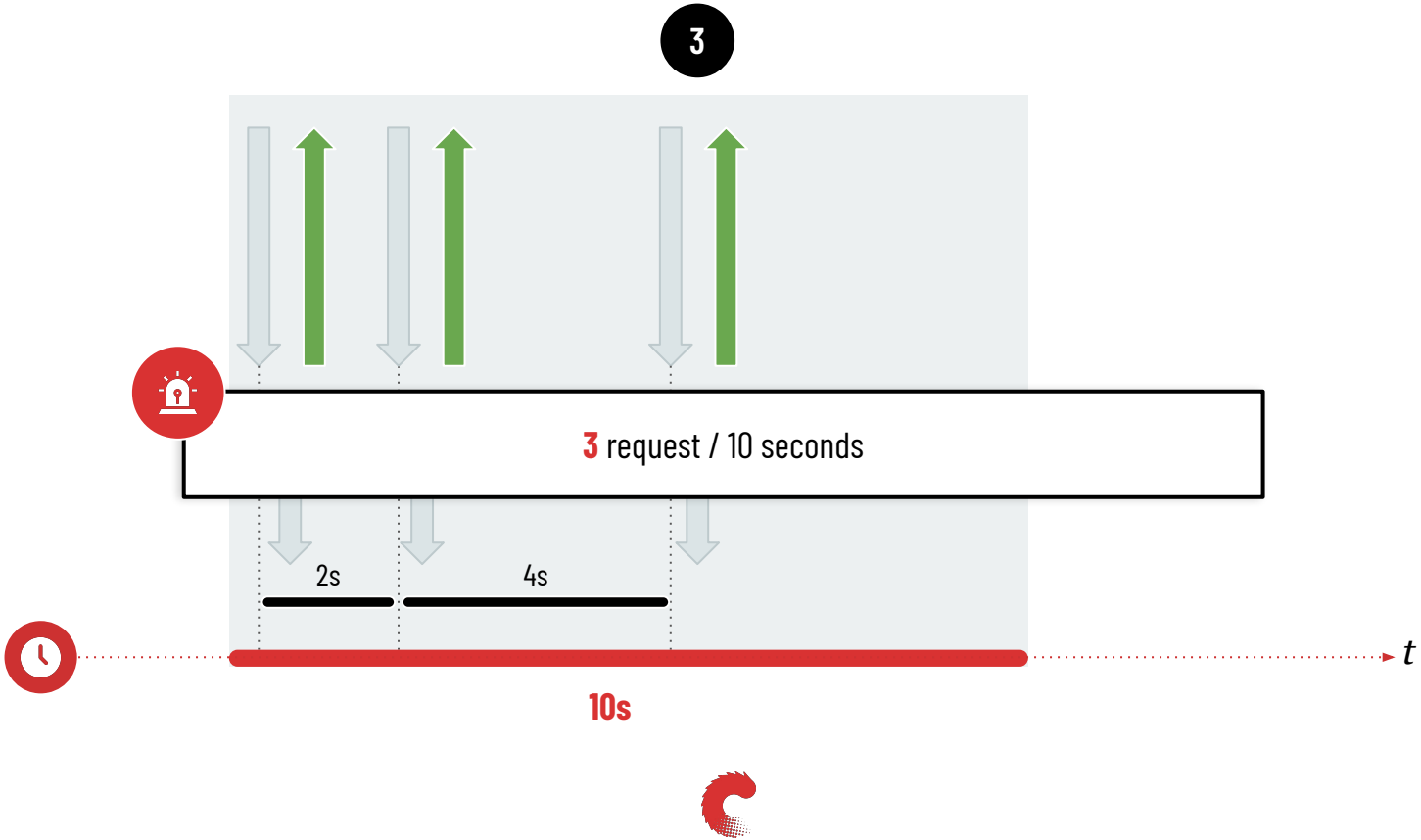
Tipologie di Rate limiting - Fixed window limit



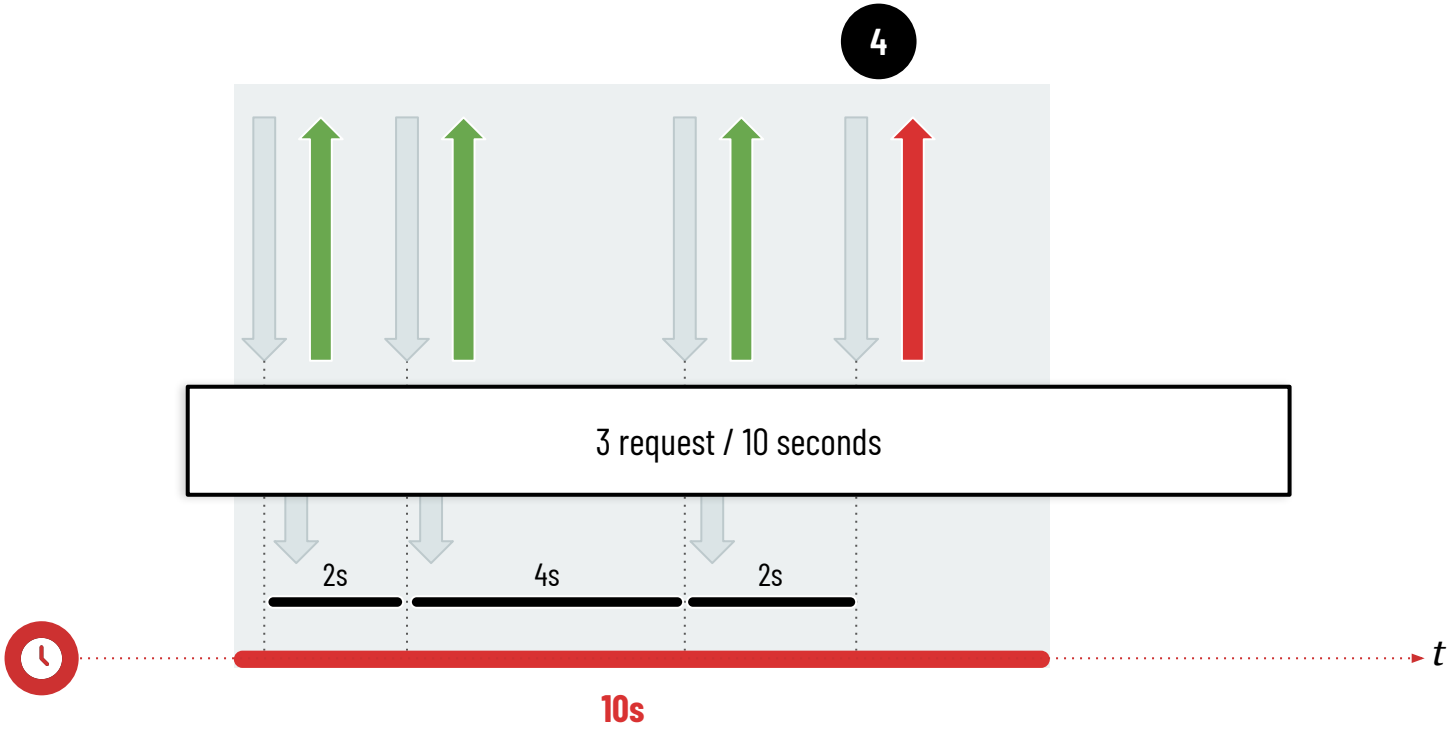
Tipologie di Rate limiting - Fixed window limit



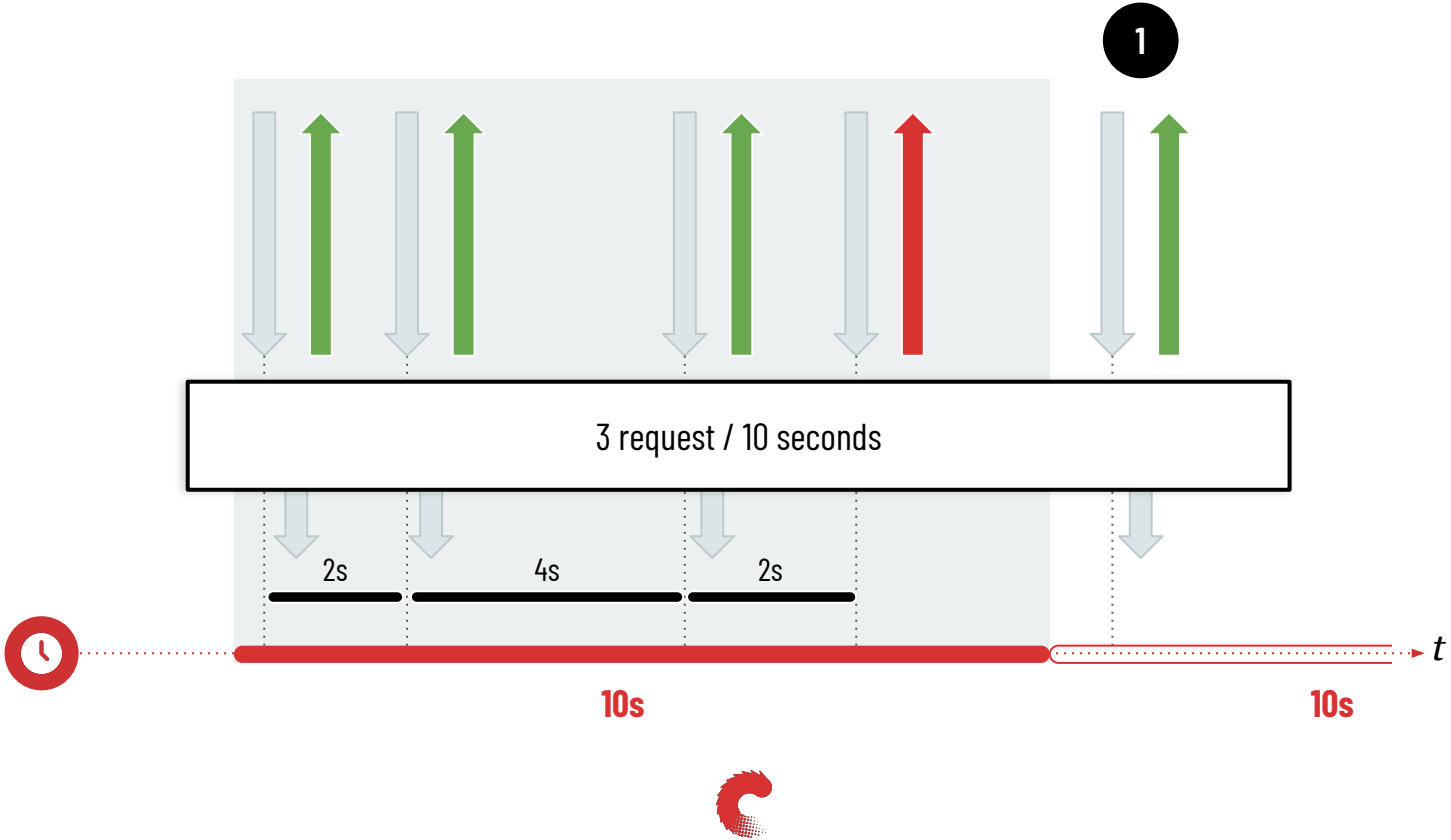
Tipologie di Rate limiting - Fixed window limit



Tipologie di Rate limiting - Fixed window limit



Tipologie di Rate limiting - Fixed window limit



Tipologie di Rate limiting - Fixed window limit

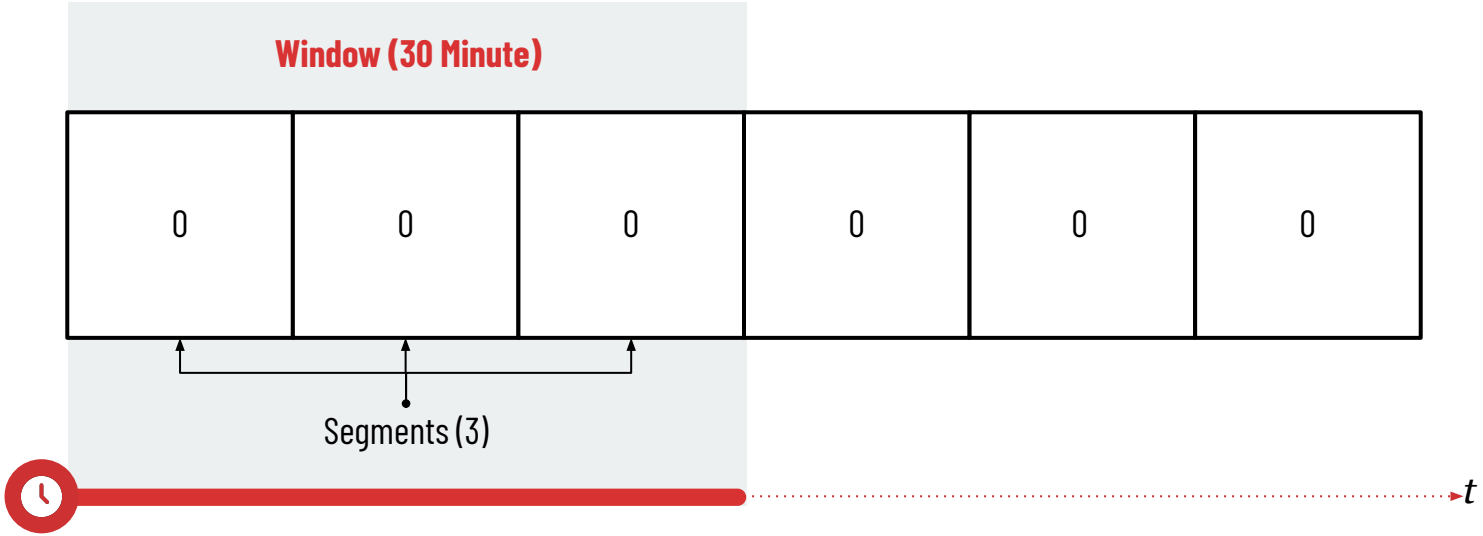
- Un singolo burst all'inizio finestra rende inutilizzabili le api per tutta la finestra
- In caso di burst in concomitanza del replenish abbiamo teoricamente raddoppiato il limite
- Molto utile per creare piani di utilizzo

Tipologie di Rate Limiter

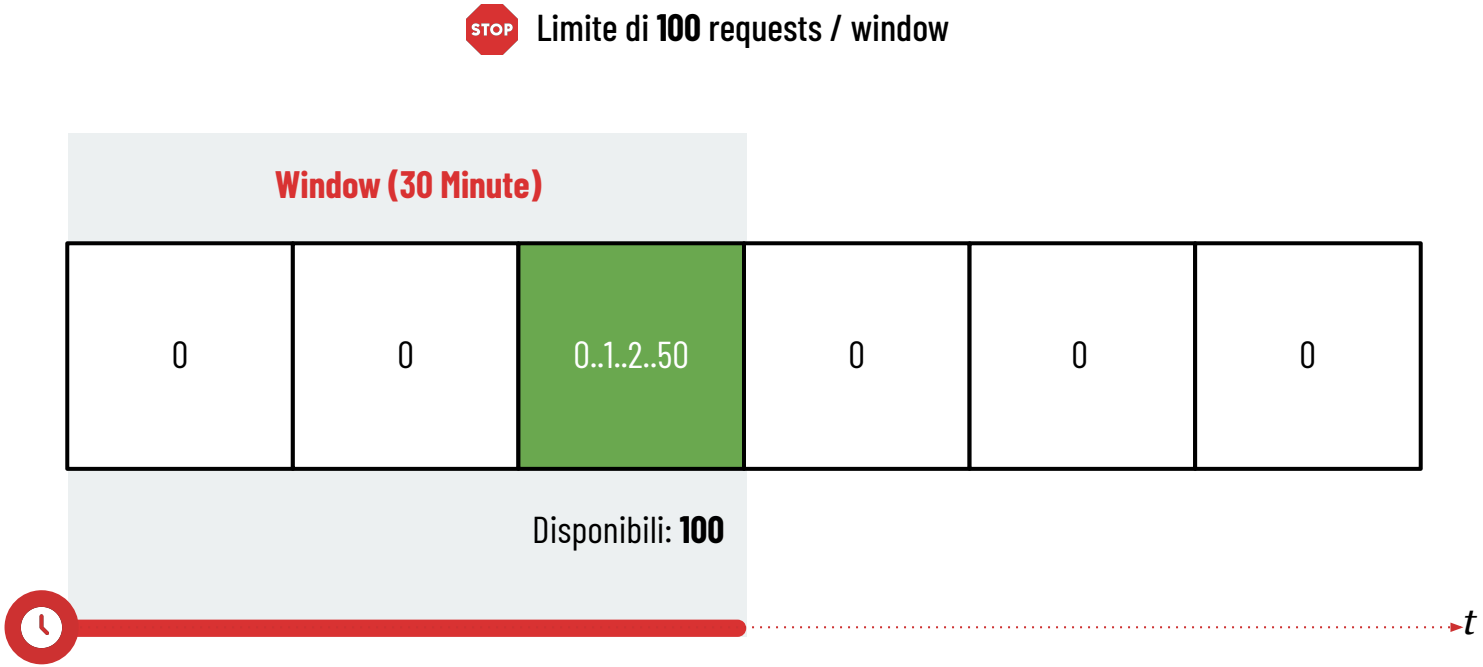
Concurrent Limit	Time Window Limit	**Sliding Window Limit**	Token Bucket Limit

Tipologie di Rate limiting - Sliding window limit

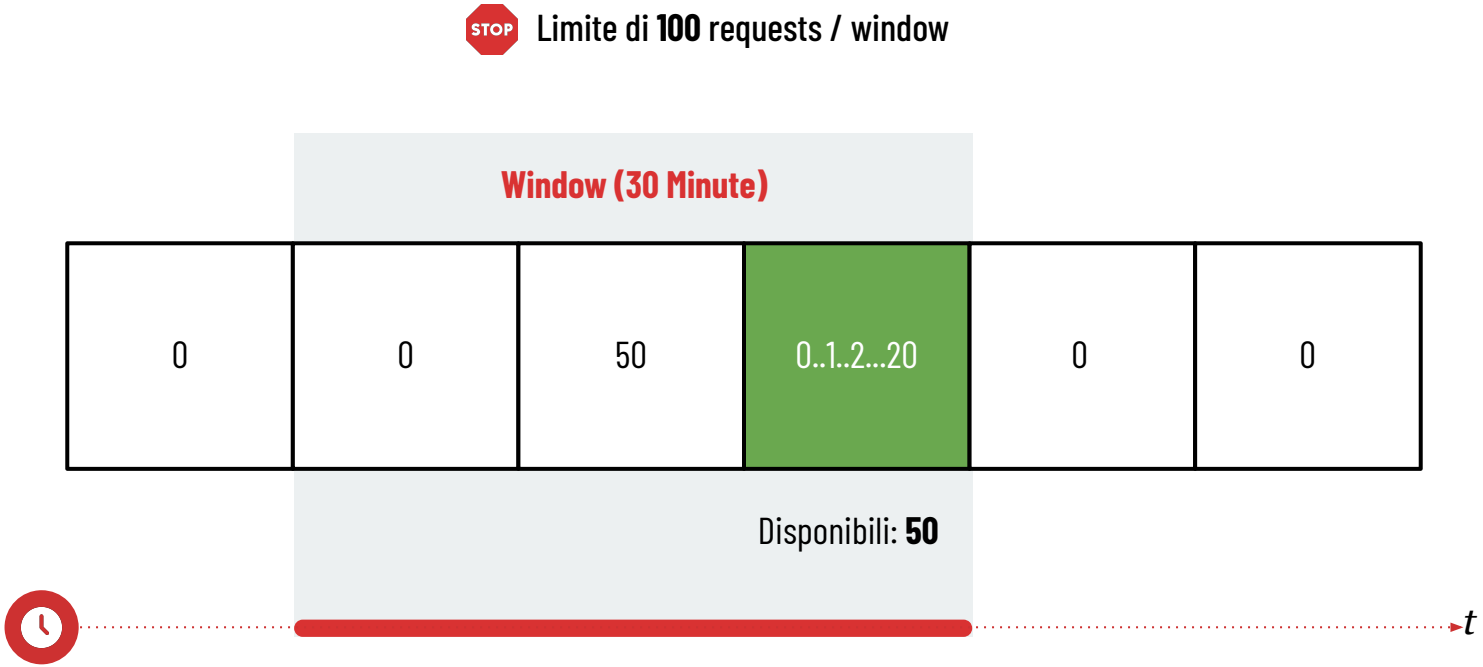
Limite di **100** requests / window



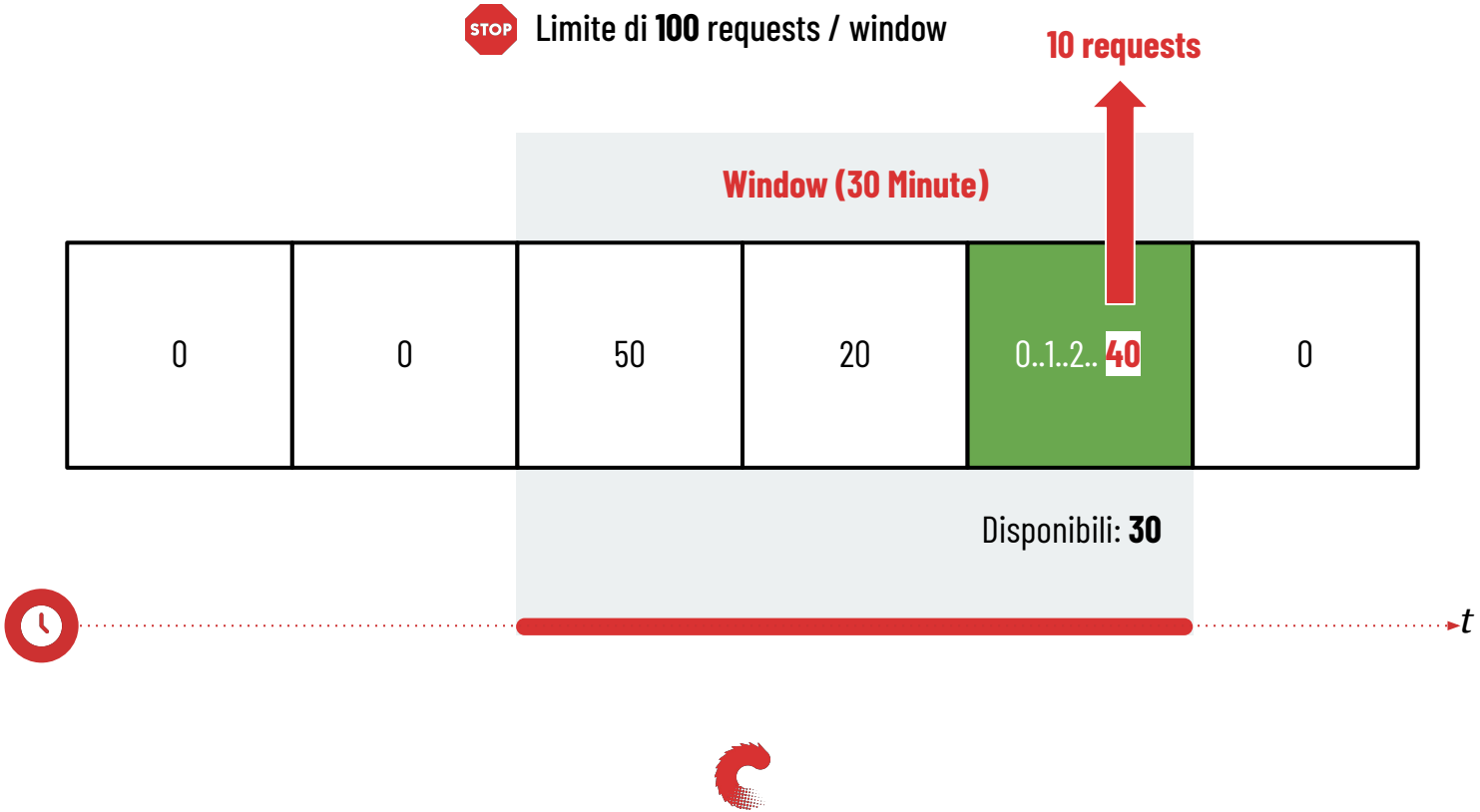
Tipologie di Rate limiting - Sliding window limit



Tipologie di Rate limiting - Sliding window limit

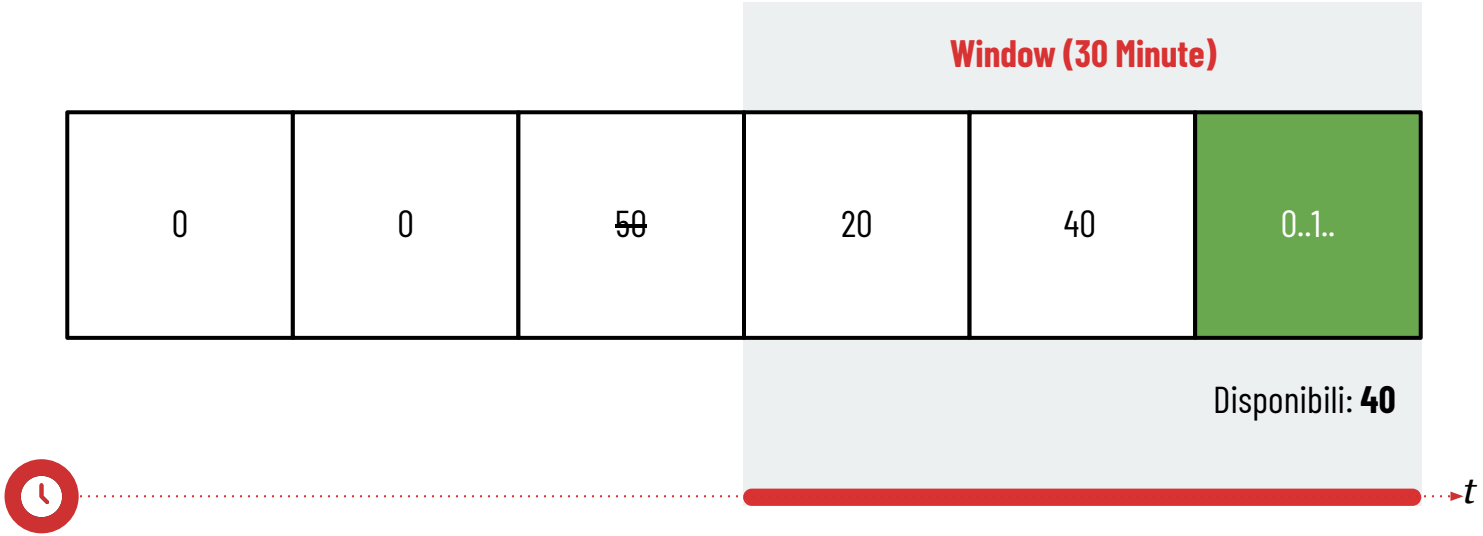


Tipologie di Rate limiting - Sliding window limit



Tipologie di Rate limiting - Sliding window limit

Limite di **100** requests / window



Tipologie di Rate limiting - Sliding window limit

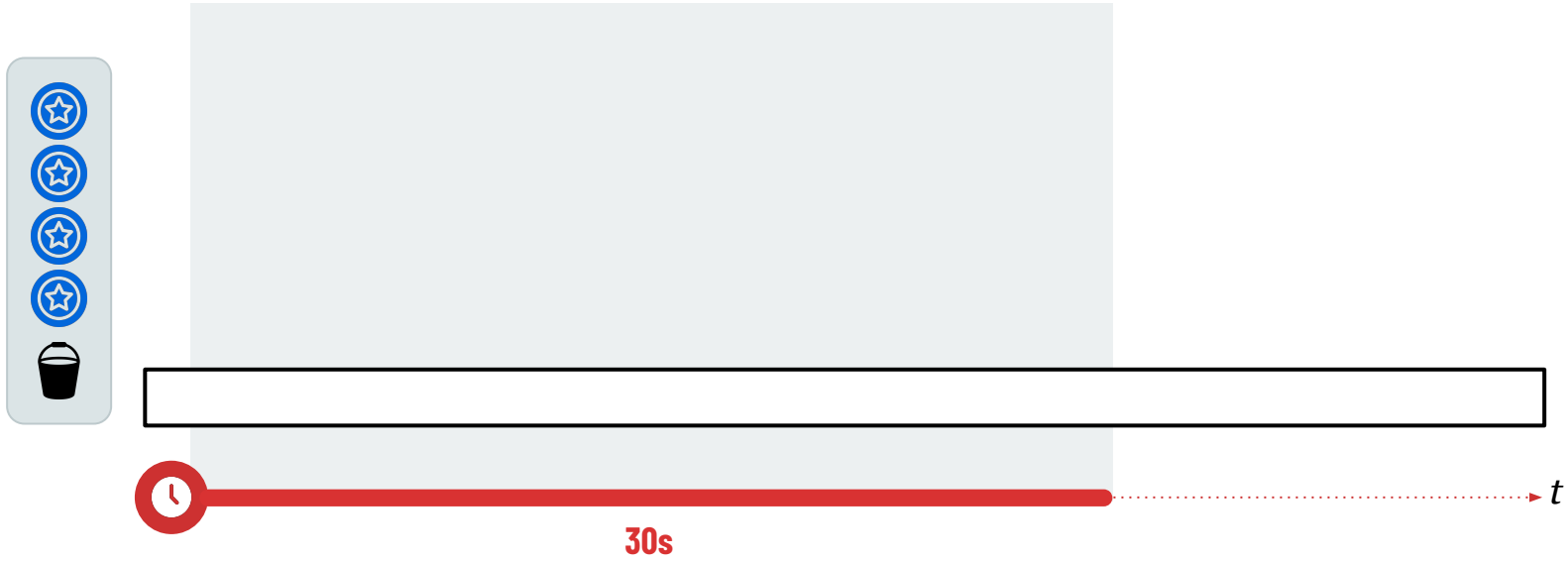
- Risolve il problema dei burst al limite della finestra del fixed window
- Penalizza i burst

Tipologie di Rate Limiter

Concurrent Limit	Time Window Limit	Sliding Window Limit	**Token Bucket Limit**

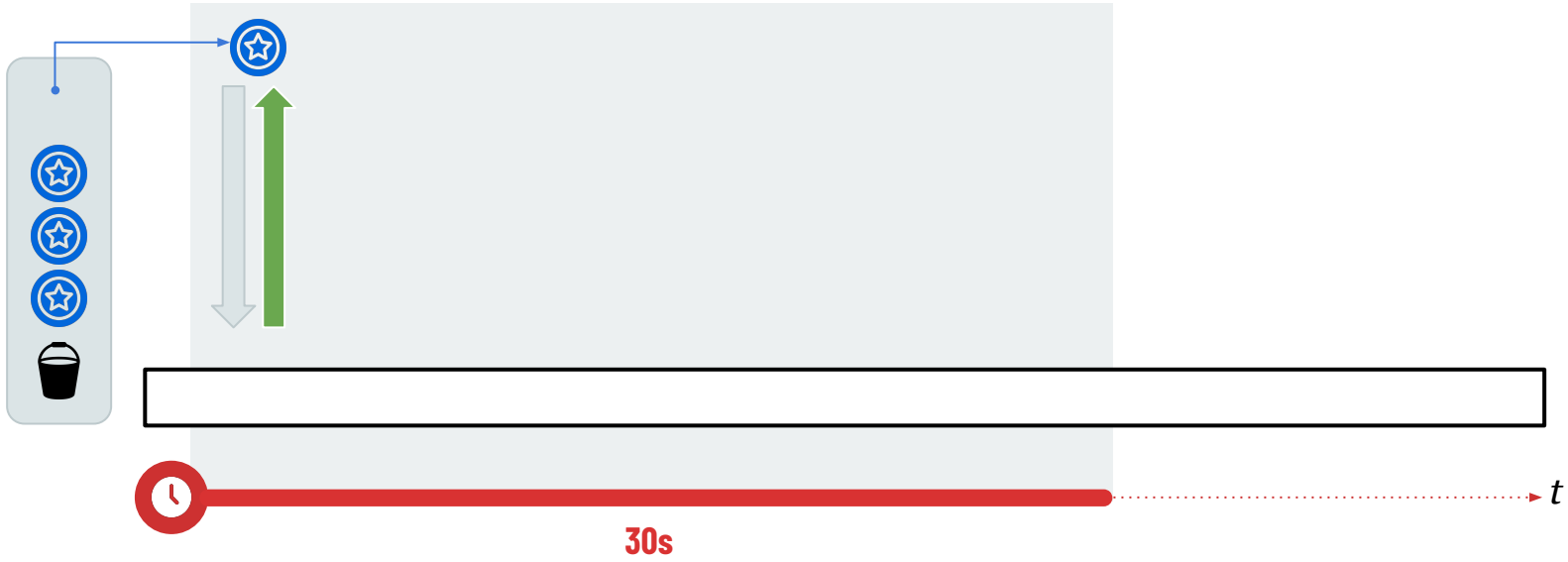
Tipologie di Rate limiting - Token bucket limit

Tokens: **4** - Periodo inserimento nuovi token: **30s** - Numero nuovi token inseriti: **1**



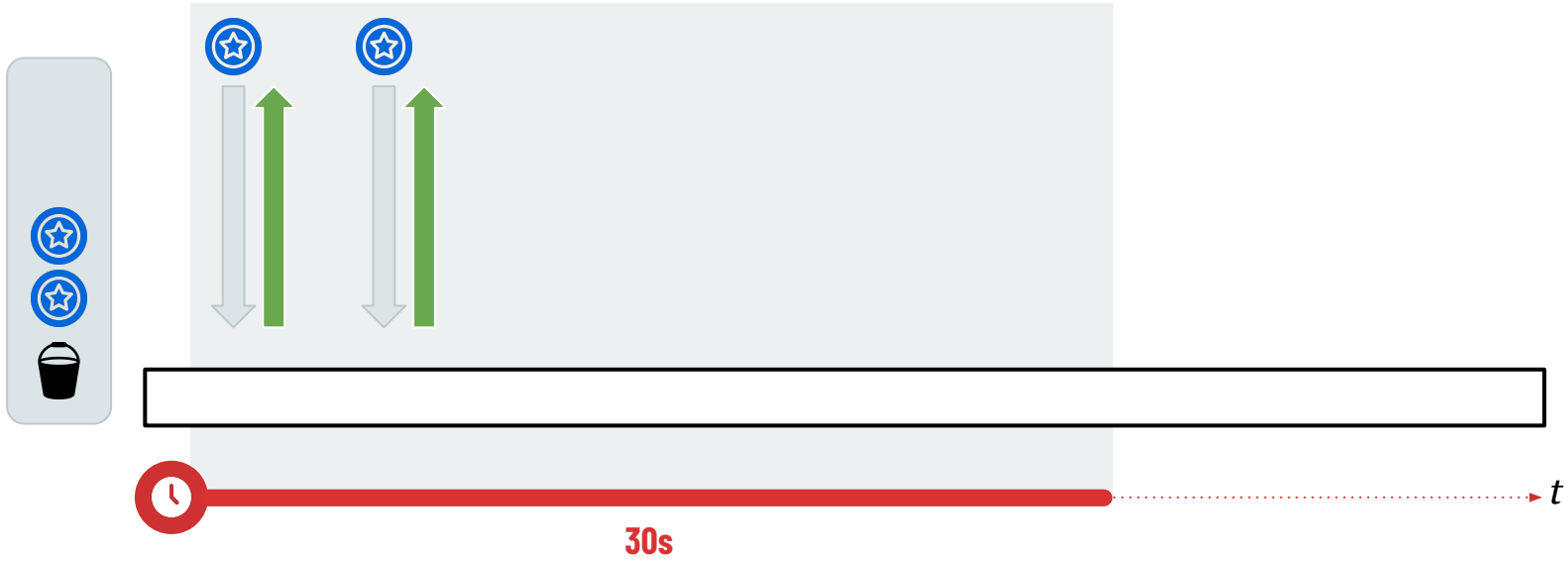
Tipologie di Rate limiting - Token bucket limit

Tokens: **4** - Periodo inserimento nuovi token: **30s** - Numero nuovi token inseriti: **1**



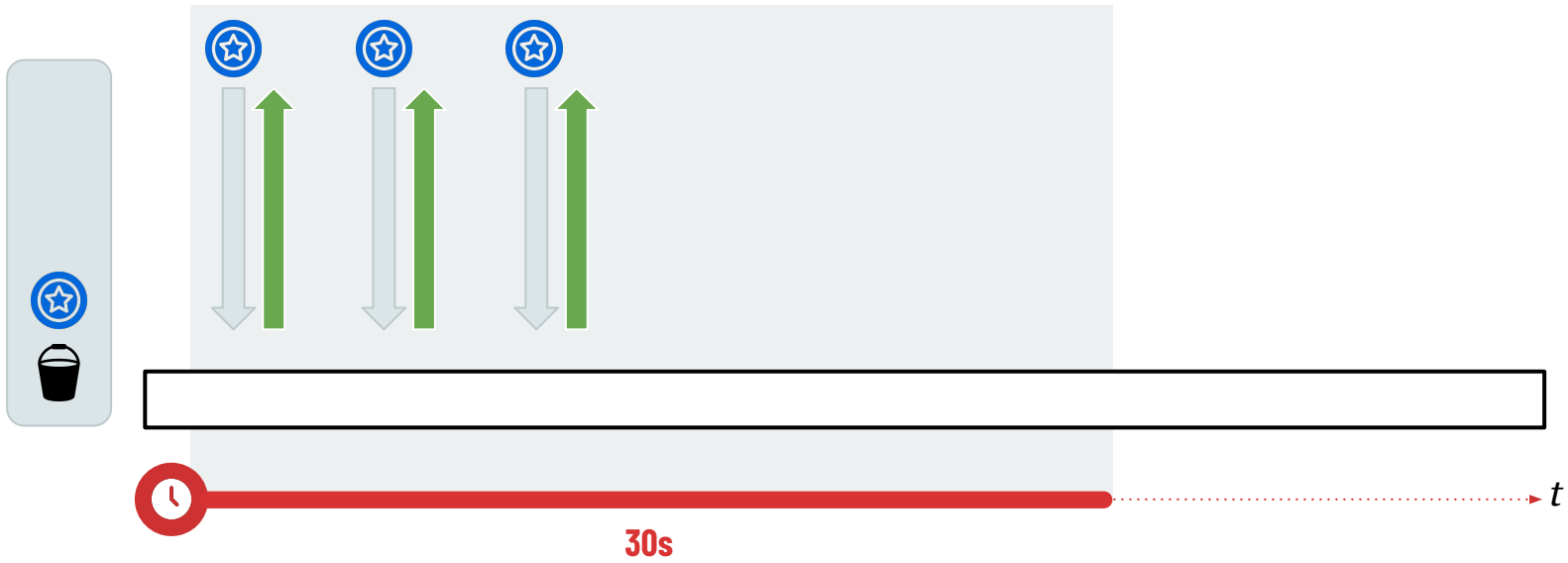
Tipologie di Rate limiting - Token bucket limit

Tokens: **4** - Periodo inserimento nuovi token: **30s** - Numero nuovi token inseriti: **1**



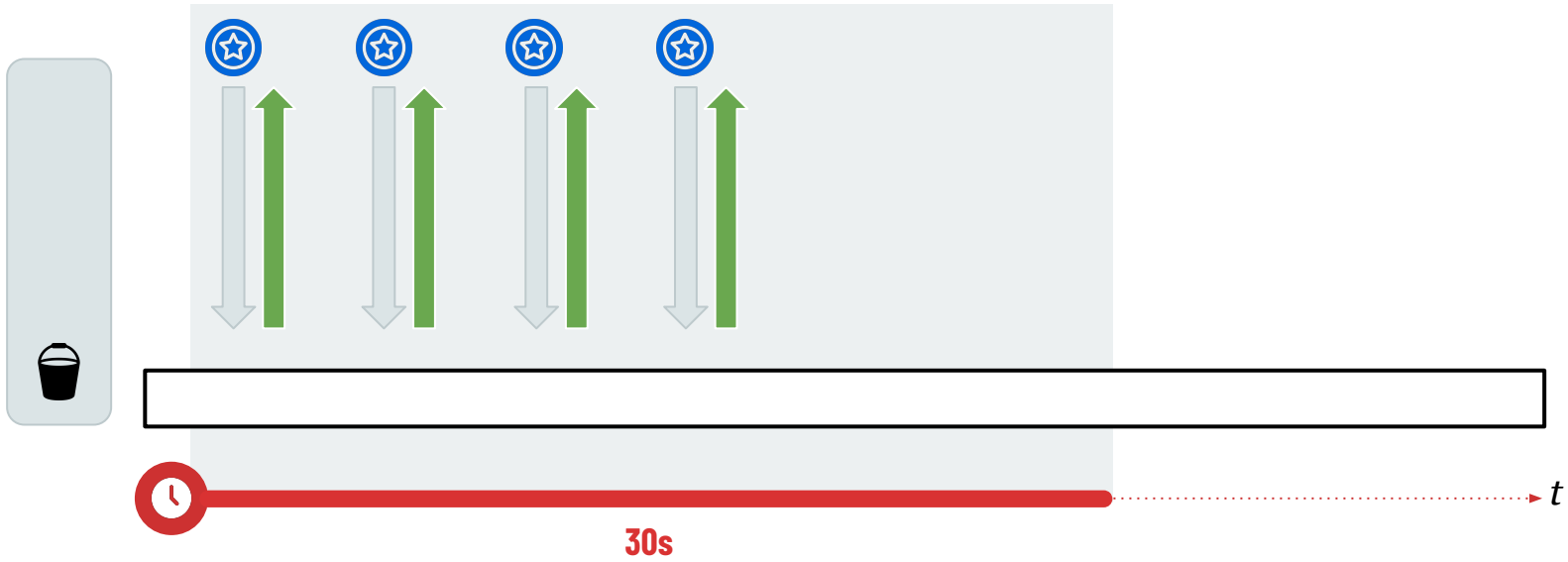
Tipologie di Rate limiting - Token bucket limit

Tokens: **4** - Periodo inserimento nuovi token: **30s** - Numero nuovi token inseriti: **1**



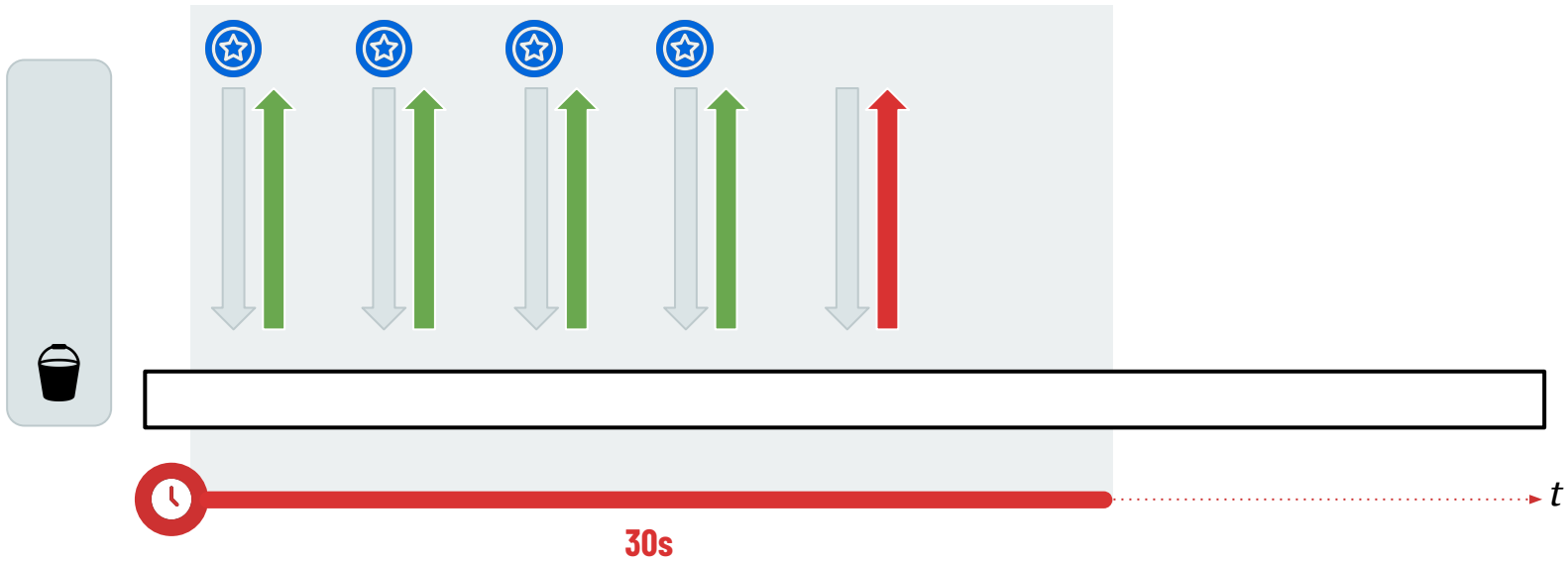
Tipologie di Rate limiting - Token bucket limit

Tokens: **4** - Periodo inserimento nuovi token: **30s** - Numero nuovi token inseriti: **1**



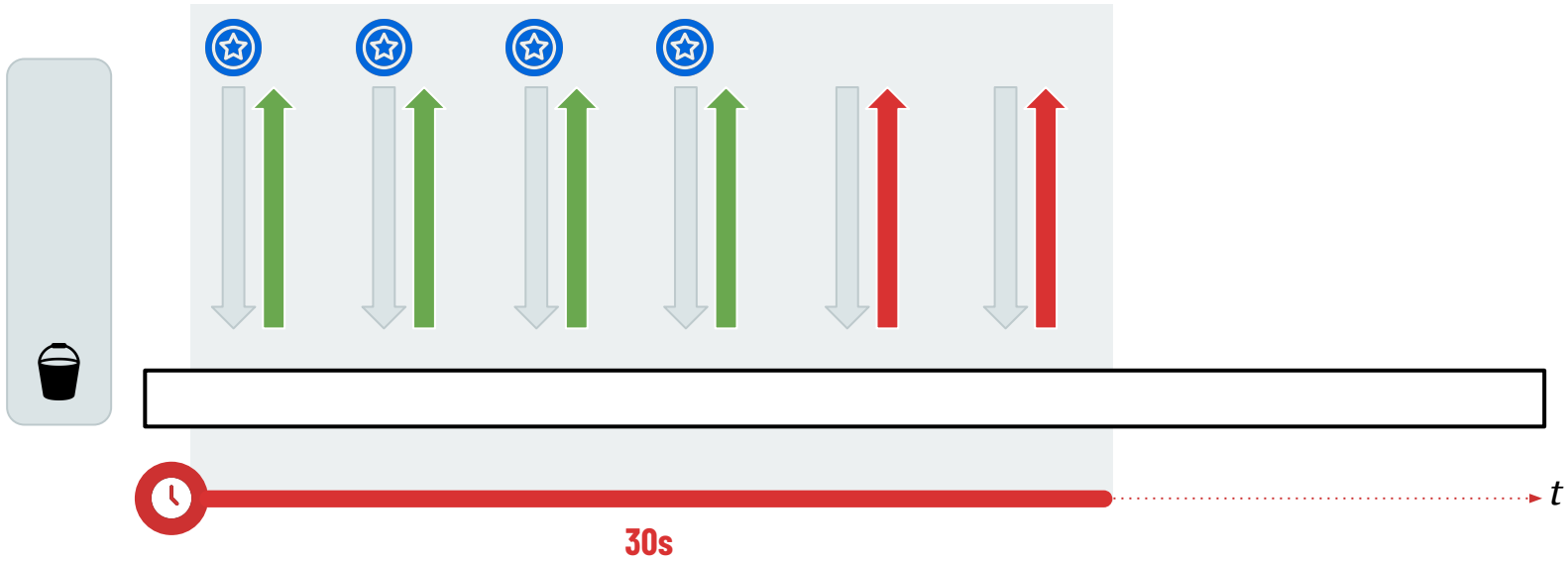
Tipologie di Rate limiting - Token bucket limit

Tokens: **4** - Periodo inserimento nuovi token: **30s** - Numero nuovi token inseriti: **1**



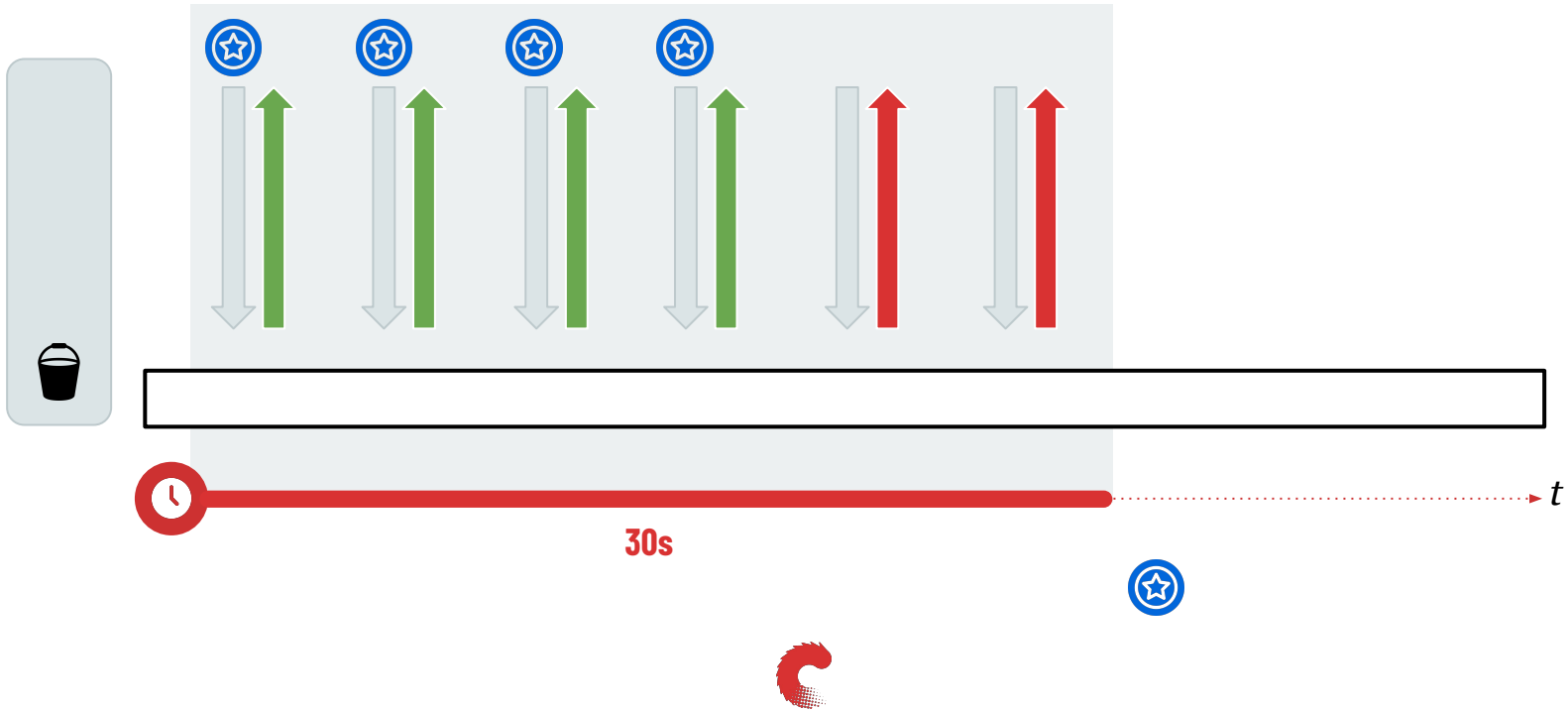
Tipologie di Rate limiting - Token bucket limit

Tokens: **4** - Periodo inserimento nuovi token: **30s** - Numero nuovi token inseriti: **1**



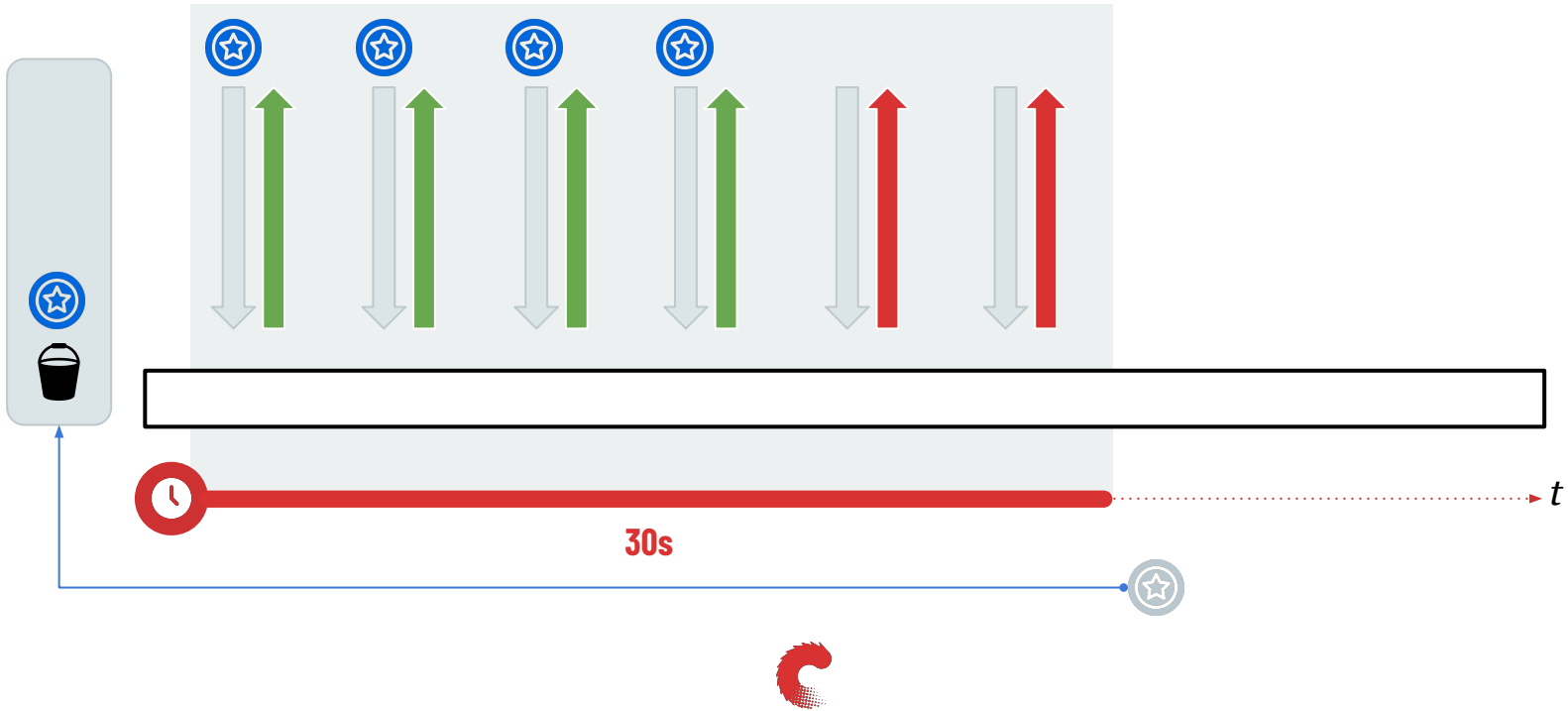
Tipologie di Rate limiting - Token bucket limit

Tokens: **4** - Periodo inserimento nuovi token: **30s** - Numero nuovi token inseriti: **1**



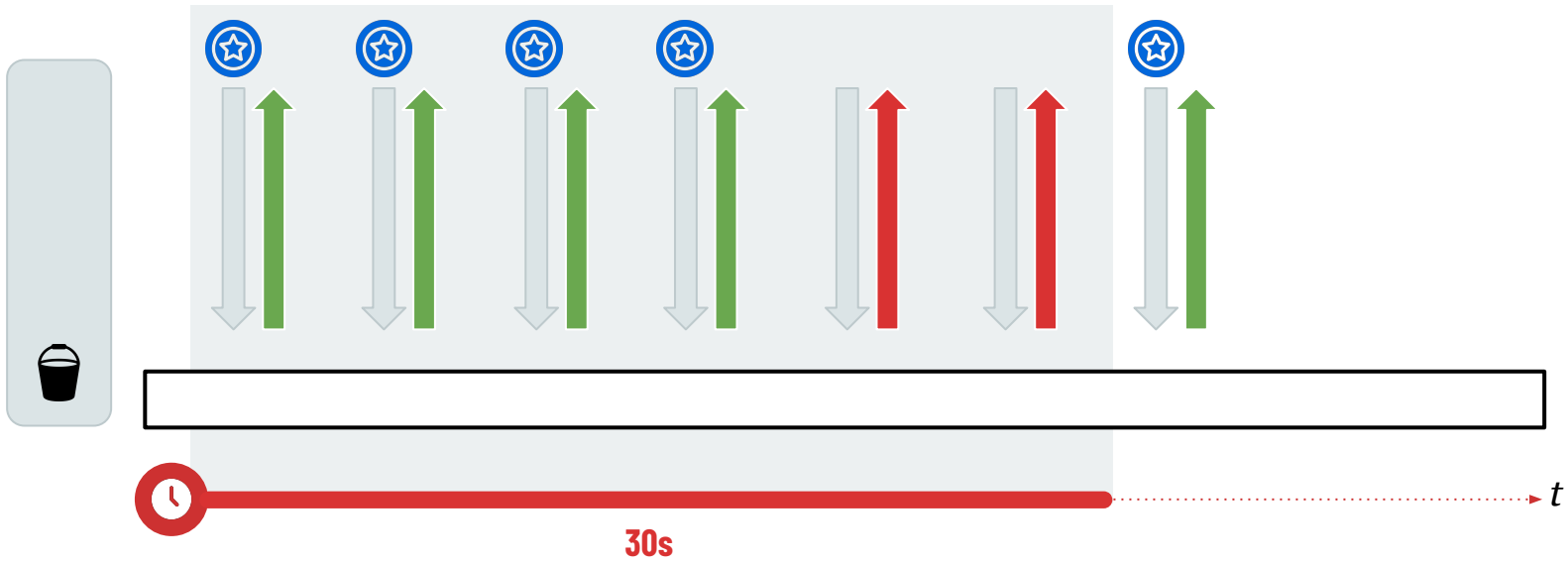
Tipologie di Rate limiting - Token bucket limit

Tokens: **4** - Periodo inserimento nuovi token: **30s** - Numero nuovi token inseriti: **1**



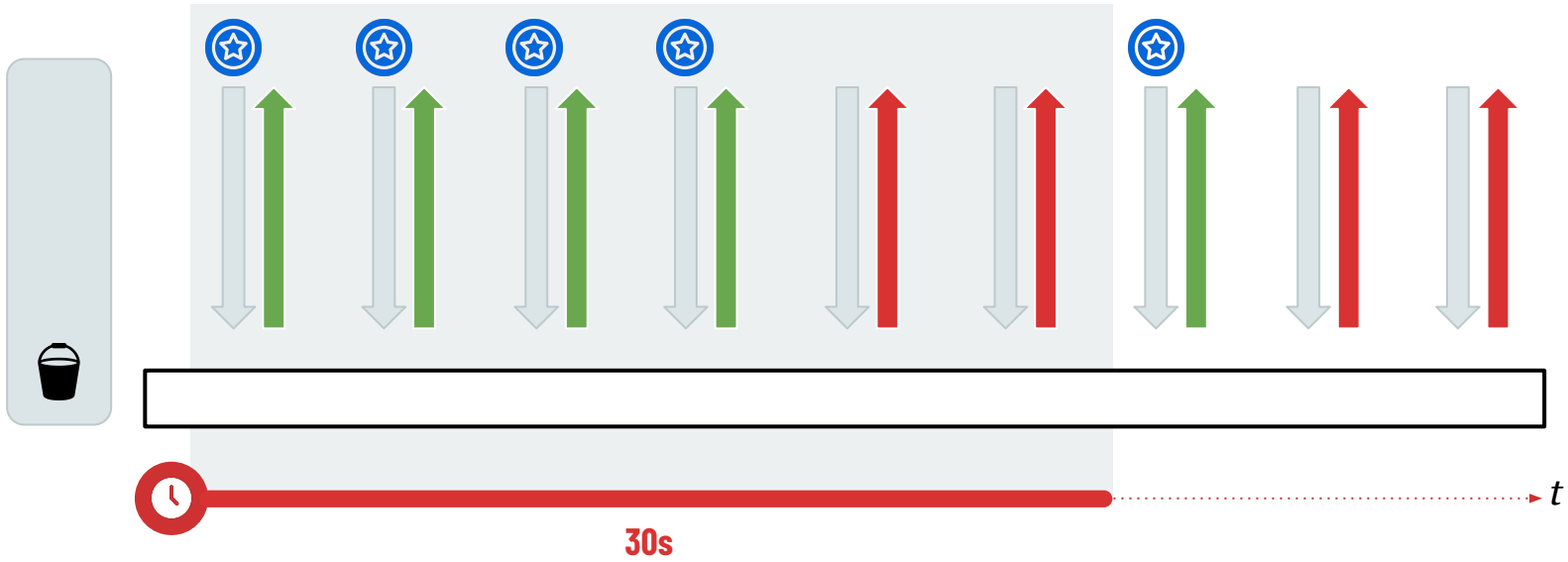
Tipologie di Rate limiting - Token bucket limit

Tokens: **4** - Periodo inserimento nuovi token: **30s** - Numero nuovi token inseriti: **1**



Tipologie di Rate limiting - Token bucket limit

Tokens: **4** - Periodo inserimento nuovi token: **30s** - Numero nuovi token inseriti: **1**



Tipologie di Rate limiting - Token bucket limit

- Incentiva un utilizzo regolare delle api
- Penalizza fortemente i burst, perchè torno alla capacità iniziale poco alla volta

.NET 6

AspNetCoreRateLimit 5.0.0

stefanprodan

.NET 7

Announcing Rate Limiting for .NET

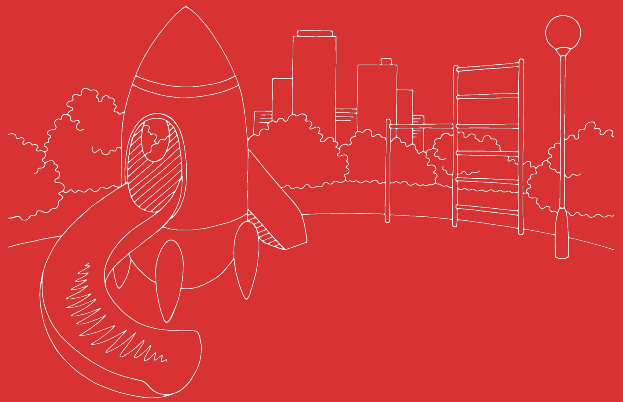
Brennan Conroy

July 13th, 2022 | 25 | 10

We're excited to announce built-in Rate Limiting support as part of .NET 7. Rate limiting provides a way to protect a resource in order to avoid overwhelming your app and keep traffic at a safe level.

AspNetCoreRateLimit 5.0.0

stefanprodan



DEMO

RateLimiterSamples.BuildInLimiters

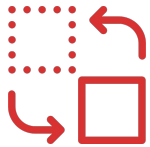
- Concurrent limit
- Time window limit
- Sliding window limit
- Token bucket limit
- Custom Policy
- Group Rate limit

RateLimiterSamples.BuildInLimiters.Mvc

- Ratelimit & MVC... il problema dell'ordine di registrazione


SCENARI AVANZATI...

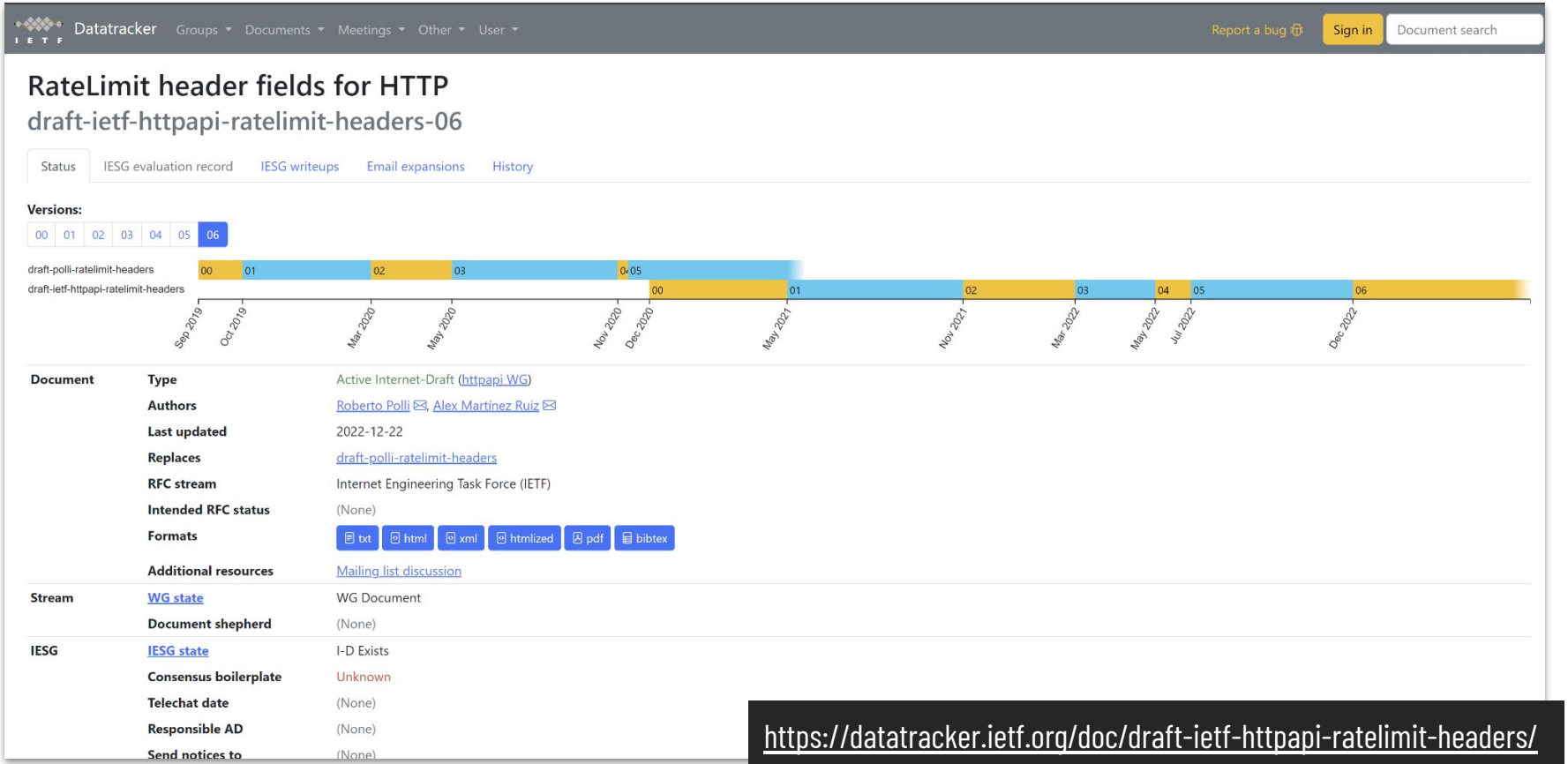
Come possiamo non sprecare chiamate?



Il client **conosce**
le policy del rate limit

Le API **condividono** lo stato
Del rate limit

Le API condividono lo stato del rate limit



https://datatracker.ietf.org/doc/draft-ietf-httpapi-ratelimit-headers/

Le API condividono lo stato del rate limit

Cosa vorrebbe l'RFC...

- **RateLimit-Limit** – to communicate the total quota within a time window.
- **RateLimit-Remaining** – to communicate the remaining quota within the current time window.
- **RateLimit-Reset** – to communicate the time (in seconds) remaining in the current time window.
- **RateLimit-Policy** – to communicate the overall quota policy.

Le API condividono lo stato del rate limit

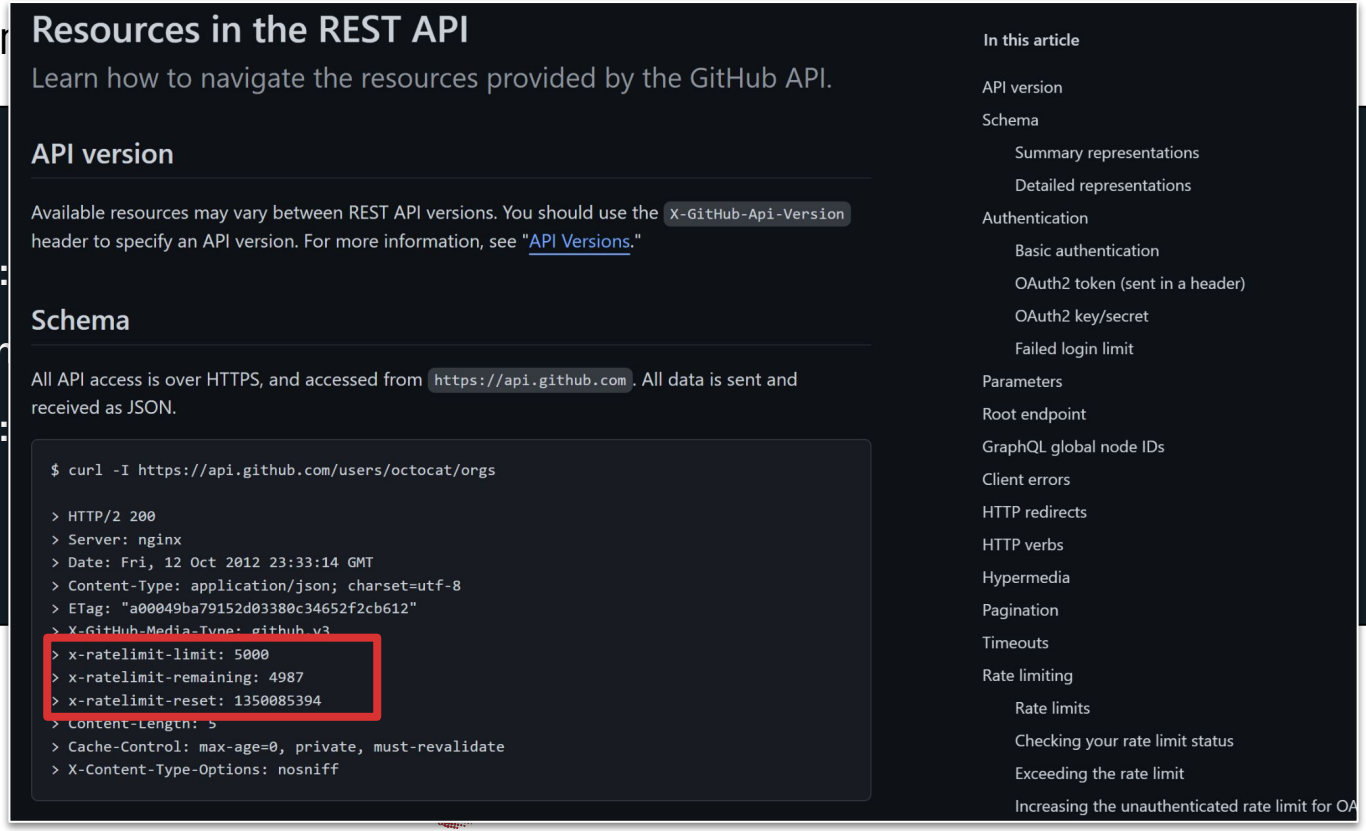
Cosa ci mette a disposizione la libreria **AspNetCoreRateLimit**...

```
X-Rate-Limit-Limit: 10s

X-Rate-Limit-Remaining: 4

X-Rate-Limit-Reset: 2022-07-24T11:30:47.2291052Z
```

Le API condividono lo stato del rate limit

Cosa ci mette a disposizion

```
X-Rate-Limit-Limit:
X-Rate-Limit-Remair
X-Rate-Limit-Reset:
```



Resources in the REST API

Learn how to navigate the resources provided by the GitHub API.

API version

Available resources may vary between REST API versions. You should use the `X-GitHub-Api-Version` header to specify an API version. For more information, see "API Versions."

Schema

All API access is over HTTPS, and accessed from `https://api.github.com`. All data is sent and received as JSON.

```
$ curl -I https://api.github.com/users/octocat/orgs

> HTTP/2 200
> Server: nginx
> Date: Fri, 12 Oct 2012 23:33:14 GMT
> Content-Type: application/json; charset=utf-8
> ETag: "a00049ba79152d03380c34652f2cb612"
> X-GitHub-Media-Type: github.v3
> x-ratelimit-limit: 5000
> x-ratelimit-remaining: 4987
> x-ratelimit-reset: 1350085394
> Content-Length: 5
> Cache-Control: max-age=0, private, must-revalidate
> X-Content-Type-Options: nosniff
```

In this article

- API version
- Schema
  - Summary representations
  - Detailed representations
- Authentication
  - Basic authentication
  - OAuth2 token (sent in a header)
  - OAuth2 key/secret
  - Failed login limit
- Parameters
- Root endpoint
- GraphQL global node IDs
- Client errors
- HTTP redirects
- HTTP verbs
- Hypermedia
- Pagination
- Timeouts
- Rate limiting
  - Rate limits
  - Checking your rate limit status
  - Exceeding the rate limit
  - Increasing the unauthenticated rate limit for OA

Le API condividono lo stato del rate limit

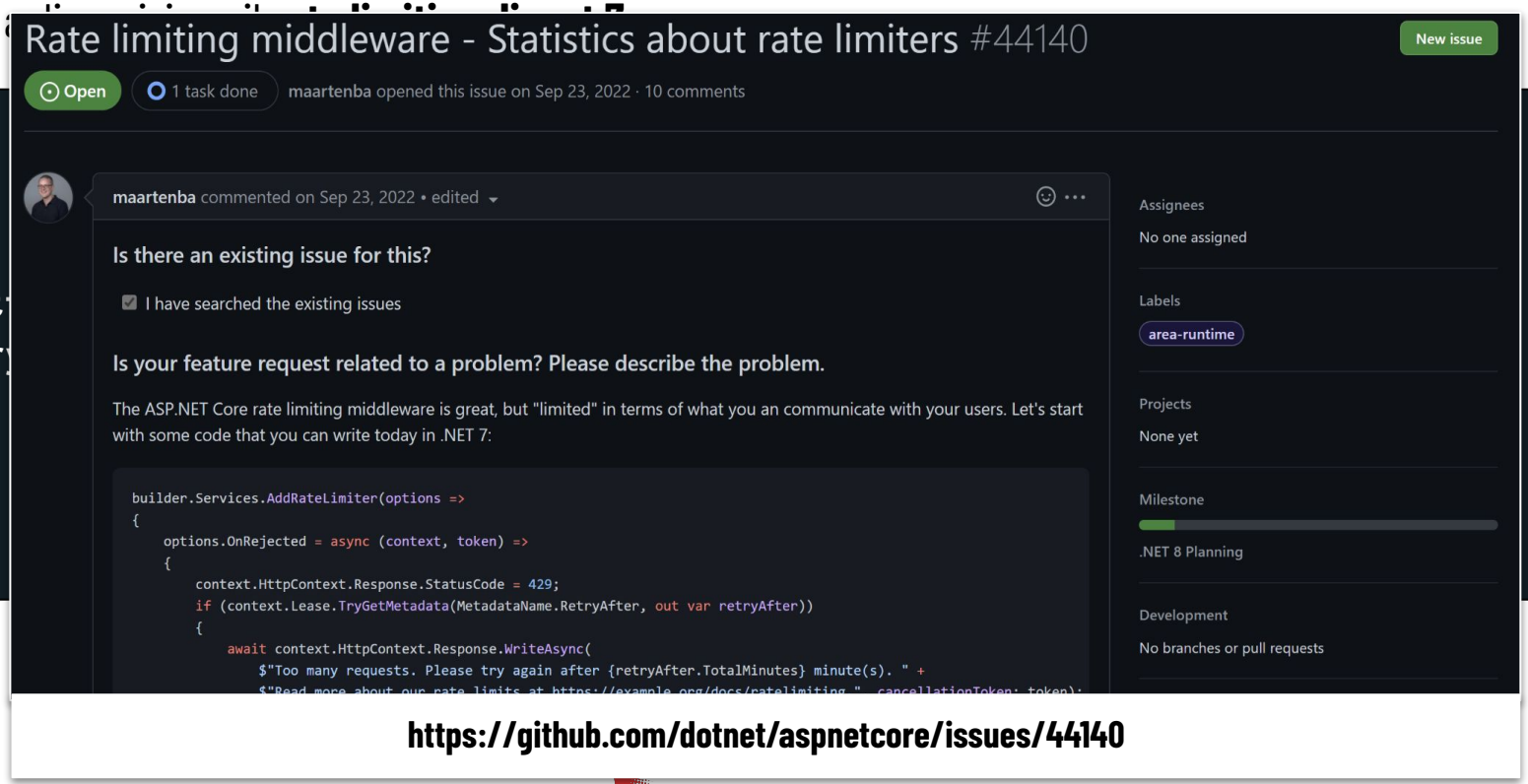
Cosa ci mette a disposizione il **rate limiting di .net 7...**

```
context.HttpContext.Response.Headers.RetryAfter =
((int)retryAfter.TotalSeconds).ToString(NumberFormatInfo.InvariantInfo);
```

Le API condividono lo stato del rate limit

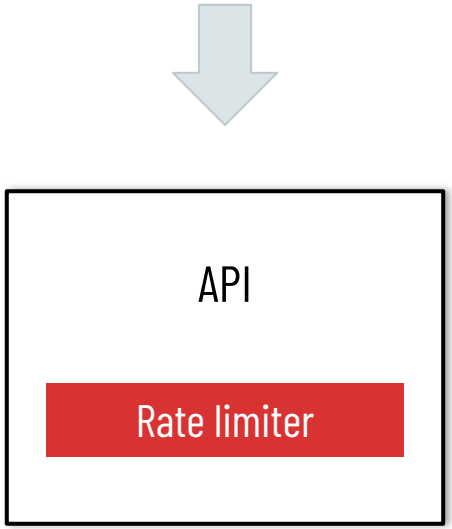
Cosa ci mette a

```
context.Ht
((int)retr
```

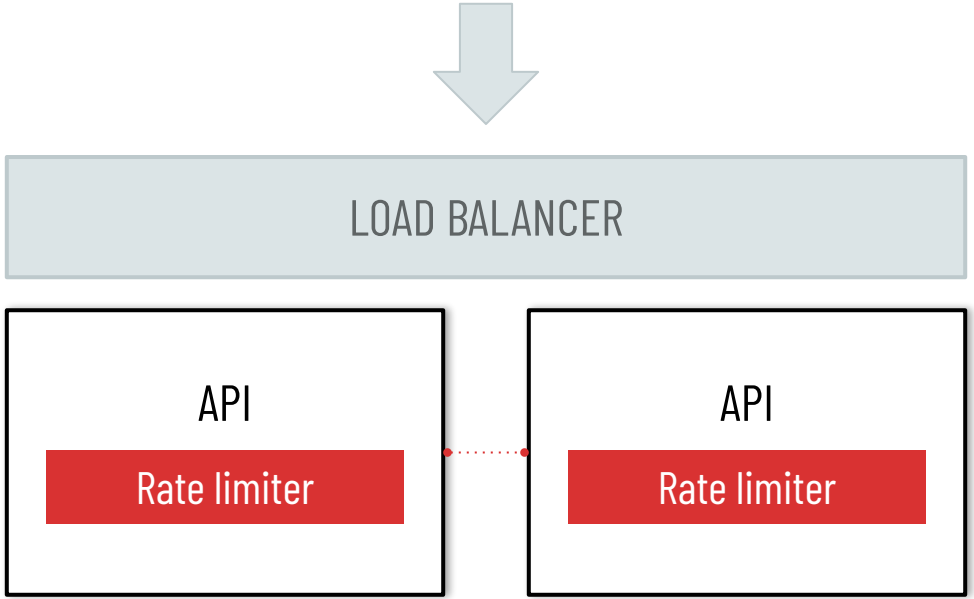


https://github.com/dotnet/aspnetcore/issues/44140

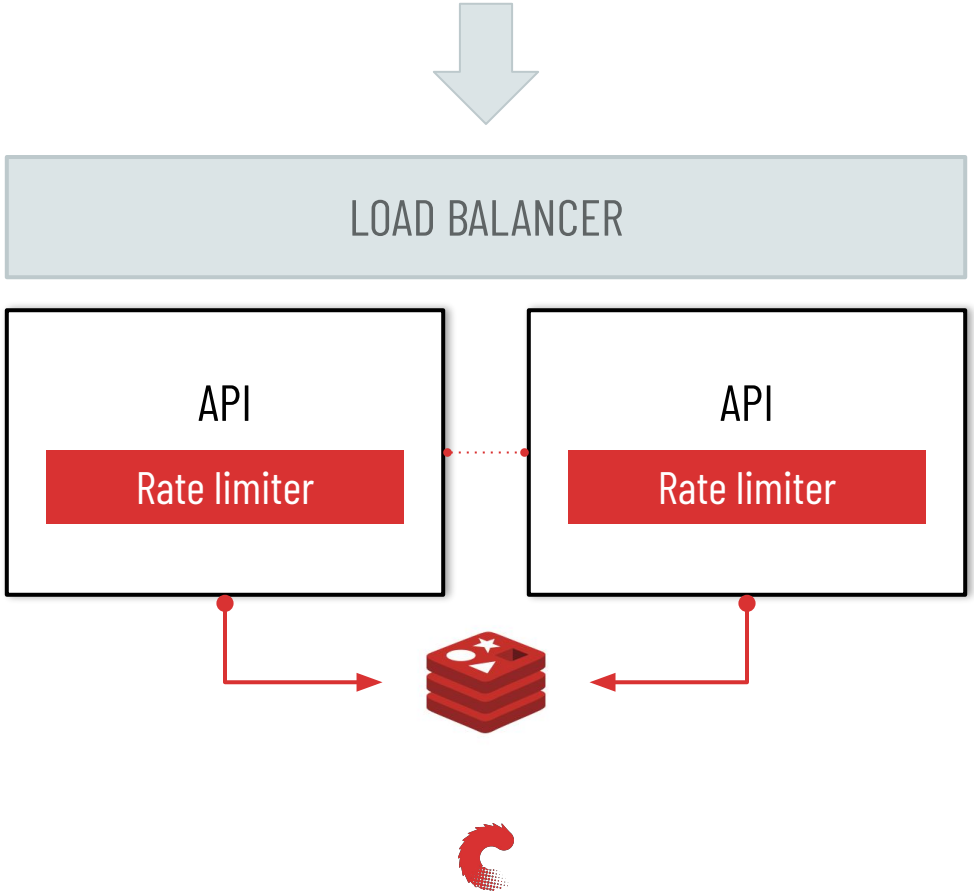
Finchè siamo “piccoli”...



..ma se il business cresce...



..ma se il business cresce...



..ma se il business cresce...

RedisRateLimiting.AspNetCore 1.0.7

.NET 7.0

.NET CLI | Package Manager | PackageReference | Paket CLI | Script & Interactive | Cake

```
<PackageReference Include="RedisRateLimiting.AspNetCore" Version="1.0.7" />
```

For projects that support PackageReference, copy this XML node into the project file to reference the package.

README | Frameworks | Dependencies | Used By | **Versions**

Version	Downloads	Last updated
1.0.7	1.702	2 months ago
1.0.6	282	3 months ago
1.0.5	137	3 months ago
1.0.4	154	3 months ago
1.0.3	56	3 months ago
1.0.2	109	3 months ago

Downloads Full stats →

Total **2.4K**

Current version **1.7K**

Per day average **24**

About

Last updated 2 months ago

Project website

Source repository

MIT license

Download package (20.12 KB)

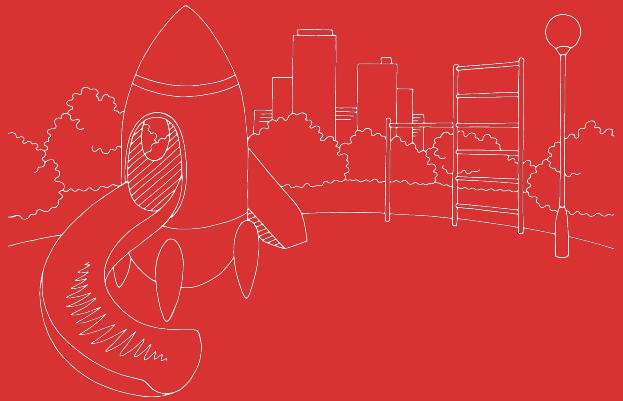
Open in NuGet Package Explorer

Open in FuGet Package Explorer

Report package

Owners Contact owners →

CP cristipufu



DEMO

- AspNetCoreRateLimit
- Client side rate limiting
- Rate limiting with Redis

Considerazioni

Incrementano **Complessità** e **dipendenze** del progetto

Considerazioni

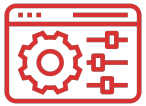
Incrementano **Complessità** e **dipendenze** del progetto

Diamo **priorità** alla protezione delle **risorse** più **onerose**

Considerazioni

Incrementano **Complessità** e **dipendenze** del progetto

Diamo **priorità** alla protezione delle **risorse** più **onerose**

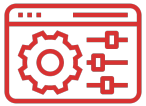


Rendere **esplicite** le policy

Considerazioni

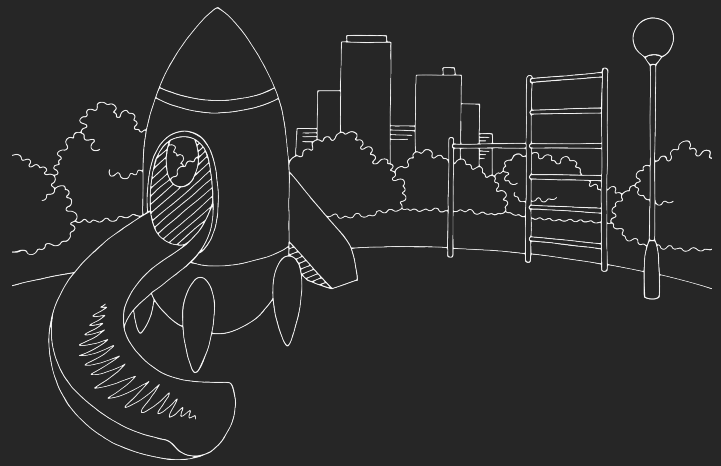
Incrementano **Complessità** e **dipendenze** del progetto

Diamo **priorità** alla protezione delle **risorse** più **onerose**



Rendere **esplicite** le policy

Non è solo per i grandi player: questa feature potrebbe **salvarci la vita** a breve!



https://github.com/GianniBortoloBossini/secure-your-api-with-rate-limiting

Materiale

- Announcing Rate Limiting for .NET
  https://devblogs.microsoft.com/dotnet/announcing-rate-limiting-for-dotnet
- API Throttling and Rate Limiting: What's the Difference?
  https://www.achieveinternet.com/post/api-throttling-vs-rate-limiting
- Different Algorithms to Implement Rate Limiting in APIs
  https://nordicapis.com/different-algorithms-to-implement-rate-limiting-in-apis
- What is a rate limiter?
  https://builtin.com/software-engineering-perspectives/rate-limiter
- Design API rate limiter
  https://www.enjoyalgorithms.com/blog/design-api-rate-limiter
- Rate limiting with token bucket
  https://blog.bagdemir.com/Rate-Limiting-with-Token-Buckets
- AspNetCoreRateLimit
  https://github.com/stefanprodan/AspNetCoreRateLimit
- Polly Rate-Limiting with ASP.NET Core
  https://github.com/martincostello/polly-rate-limiting

Materiale

- Polly - Rate-Limit
  https://github.com/App-vNext/Polly#rate-limit
- ASP.NET Core rate limiting middleware in .NET 7
  https://blog.maartenballiauw.be/post/2022/09/26/aspnet-core-rate-limiting-middleware.html
- Rate limit an HTTP handler in .NET
  https://learn.microsoft.com/en-us/dotnet/core/extensions/http-ratelimiter
- On implementing the ASP.NET Core 7 rate-limiting middleware
  https://nicolaiarocci.com/on-implementing-the-asp.net-core-7-rate-limiting-middleware
- Exploring Communication of Rate Limits in ASP.NET Core With Rate Limit Headers
  https://www.tpeczek.com/2022/07/exploring-communication-of-rate-limits.html
- Microsoft Releases New .NET Rate Limiter in .NET 7-And It's Amazing!
  https://www.bytehide.com/blog/new-microsoft-dotnet-rate-limiter-for-rate-limiting

Per altri articoli nerd (e non solo)
https://blog.codiceplastico.com

GIANNI BOSSINI

Software Engineer @ CodicePlastico

gianni.bossini@codiceplastico.com

TW @bossinigianni - **LK** giannibortolobossini

CODICEPLASTICO

ANALISI, SVILUPPO, FORMAZIONE, ASSESSMENT AZURE, UI & UX DESIGN

www.codiceplastico.com

Grazie!

FOLLOW US