04

Para saber mais: Explorando o uso de tokens

Neste curso, estamos criando um sistema de login com tokens para o Blog do Código. Dessa forma, algumas decisões de projeto levam em conta as demandas desse serviço. Entretanto, aplicações diferentes podem precisar de decisões de projeto diferentes. Assim, vamos descrever algumas modificações no projeto que podem extrair o máximo da escalabilidade dos tokens.

Remover rota de logout

Num contexto de sessões, é esperado existir uma operação de logout em conjunto com a de login. Entretanto, ao utilizar Json Web Tokens, é necessário criar uma *blocklist* para permitir essa operação e fazer consultas nessa base a cada uso do token.

Por isso, num sistema com muitos acessos, essa consulta pode sobrecarregar o servidor. Assim, pode ser interessante remover essa operação, eliminando a necessidade de consultar uma base a cada requisição, mesmo que seja em memória como o Redis.

Além disso, é possível remover essa rota e ainda simular uma operação de logout através da plataforma que consumiria a API. Por exemplo, um aplicativo mobile poderia guardar o token JWT no momento de login e, quando a pessoa executasse a operação de logout, esse token seria apagado da memória. Com isso, uma pessoa que possuísse esse token ainda poderia fazer requisições com ele mas quem estivesse usando o aplicativo da forma usual teria a ilusão de que o token foi invalidado. Ainda, o tempo de expiração do token deve ser diminuído para dificultar ataques.

Remover busca do usuário na base

No começo de toda rota que precisa de autenticação, a requisição passa por um *middleware* que verifica se a pessoa está autenticada e busca seu respectivo usuário na base, inserindo em `req.user`. Entretanto, se alguma dessas rotas tiver um fluxo de requisições muito alto e não há a necessidade de buscar as informações do usuário na base, apenas saber seu `id`, então pode ser interessante modificar esse padrão de desenvolvimento.

Assim, pode ser feito um outro *middleware* de autenticação que verifica o token e insere apenas o id na requisição. Dessa forma, essas rotas podem operar sem qualquer consulta numa base de dados.

Além disso, é possível notar o impacto de uma consulta a um banco através de alguns benchmarks. Se pegarmos um teste de requisições onde é feita uma consulta em banco (https://www.techempower.com/benchmarks/#section=data-r19&hw=ph&test=db), vemos que ela é 10 vezes mais lenta que uma requisição onde devolve-se apenas um *plaintext* (https://www.techempower.com/benchmarks/#section=data-r19&hw=ph&test=plaintext).