Podcast

Disciplina: Interface de programação de aplicações (API) e Web Services

Título do tema: Análise de Projetos de Arquiteturas de APIs e Web Services e Seleção de Tecnologias para Implementação

Autoria: Arthur Gonçalves Ferreira

Leitura crítica: Rennan Martini Rodrigues

Olá, ouvinte! No podcast de hoje vamos falar sobre Gateway API.

O API Gateway é uma interface que realiza o gerenciamento de tráfego de dados com o back-end da aplicação. O API Gateway atua também na proteção de dados valiosos através de políticas de autenticação e de controle de acesso geral para chamadas de APIs. Dessa forma, você pode entender um API Gateway como uma interface que realiza o controle de acesso de um determinado sistema e a serviços back-end, ou seja, a API Gateway cria condições mais favoráveis para a comunicação entre clientes externos e os serviços de back-end de uma aplicação, de uma forma que os clientes tenham satisfação em utilizar um determinado serviço.

Um dos grandes objetivos da API Gateway, além dos já citados aqui, é garantir que um sistema possa então suportar uma elevada carga de processos e mesmo assim conseguir manter a disponibilidade de serviços. A API Gateway encaminha uma solicitação a um determinado serviço e envia a resposta ao seu solicitante.

Para realizar a segurança de autenticação de usuário, o API Gateway pode utilizar diversas formas para reconhecimento de uma identidade ou validade de autenticação. Uma das formas seria com a utilização de meios considerados não padrões de autenticação, que realizam a autenticação no cabeçalho da mensagem. Outra forma seria a utilização de APIs de segurança como, por exemplo, o API Firewalling, que funciona realizando a validação de conteúdo e verificação de integridade de mensagens, podendo até verificar se uma API foi adulterada.

Por tanto, nós temos que o API Gateway pode ter as seguintes funções:

1. Realizar a integração de várias plataformas como, por exemplo, mobile e web e filtrar o tráfego de chamadas dessas plataformas;

2. É a única porta de entrada para usuários e APIs;

3. Atua como um roteador de tráfego das APIs;

4. Garante proteção por meio da autenticação de usuário;

5. Limitação de conexões, fazendo com que somente pessoas autorizadas possam acessar um determinado sistema;

6. Limita o acesso aos seus serviços na web a um único ponto, que seria o próprio API Gateway.

7. Auxilia na redução de custos ao manter APIs no ar.

É extremamente importante que você saiba que a API Gateway é a mesma coisa do que o serviço AWS, mais conhecido como Amazon API Gateway. Na realidade, AWS é um API Gateway da empresa Amazon, neste caso é um produto. Os conceitos relacionados ao API Gateway não estão relacionados somente a uma empresa específica, neste caso, entenda que o AWS é um produto genérico que existe no mercado, classificado como um API Gateway.

Além da AWS, existem diversas soluções de API Gateway, que podem ser proprietárias, que significa que você precisa pagar para poder utilizar, existem as API Gateway open-source e as API Gateway de nuvem. Entre as principais, temos Kong, KrakenD, IBM® Cloud API Gateway e Tyk.

Este foi nosso podcast de hoje! Até a próxima!