**Curso** MAAZARQD - Master Class de Arquitetura Microsoft Azure — Desenvolvimento

Duração: 28h

**Introdução**

A cloud é um excelente ambiente para construir aplicações resilientes, de alta disponibilidade, com bom desempenho e, com sorte, sem custos exagerados. Mas como se atingem esses objetivos? Nesta formação começamos por examinar os problemas que um programador ou arquiteto de cloud pode encontrar. Depois exploramos soluções através de padrões comprovados. Por fim, aprofundamos as várias tecnologias disponíveis no Azure para implementar esses padrões. O enfoque desta formação são conceitos e padrões aplicáveis a qualquer ambiente cloud; não entramos nos detalhes técnicos de cada recurso Azure.

**Público-alvo**

Este curso avançado destina-se a quem pretenda tornar-se arquiteto de cloud em Microsoft Azure. O objetivo é desenvolver aplicações cloud-native, com foco em PaaS (Platform as a Service), cobrindo também os temas de infraestrutura relevantes.

**No final do curso**

Após a conclusão deste curso, os formandos deverão ser capazes de:
• Desenhar aplicações cloud-native em Azure, com foco em PaaS e em microserviços.
• Escalar aplicações e bases de dados no Azure e escolher entre SQL e NoSQL.
• Definir estratégias de caching e de comunicação síncrona e assíncrona.
• Desenhar soluções de mensagens e garantir a consistência dos dados.
• Aplicar CQRS e Event Sourcing.
• Tratar a comunicação externa e as questões de segurança da arquitetura.

**Pré-requisitos**

Base sólida de desenvolvimento e bom conhecimento de Azure. Para quem pretende aprender a desenvolver em Azure, recomenda-se primeiro o curso MAAZD «Azure | Developer».

**Exames de certificação**

(não existem exames)

**Conteúdo programático em detalhe**

**Introdução à arquitetura Azure**
• A infraestrutura global do Azure
• Blocos de construção da arquitetura: aplicações, dados, comunicação e outros
• Considerações: disponibilidade, resiliência, desempenho, custo, ...
**Microserviços**
• Lidar com a evolução de uma aplicação
• Vantagens e desvantagens
• Comunicação: cliente-serviço e serviço-serviço

• Isolamento de dados

**Escalar uma aplicação no Azure**

• Usar um app service plan
• Usar um orquestrador
• Serverless
• Multirregião
• Balanceamento de carga
• Recursos do Azure: Traffic Manager, Front Door, Load Balancer e Application Gateway
• LAB: montar failover ativo/passivo

**SQL versus NoSQL**

• Schemas e relações
• Consistência de dados
• Desempenho de leitura e de escrita
• Particionamento e escalabilidade
• Recursos do Azure: Azure SQL e Cosmos DB
• LAB: desenhar uma base de dados NoSQL

**Escalar uma base de dados no Azure**

• Escalabilidade vertical vs. horizontal
• Partitioning e sharding
• Multirregião
• Recursos do Azure: Azure SQL e Cosmos DB
• LAB: recuperação de desastre com Azure SQL

**Estratégias de caching**

• Azure Redis Cache
• O padrão cache-aside
• Read-through e write-through
• O padrão materialized view
• O padrão valet key
• Azure CDN

**Comunicação síncrona**

• Retry e circuit breaker
• Throttling
• O padrão bulkhead
• O padrão ambassador
• LAB: usar o Circuit Breaker pattern

**Comunicação assíncrona**

• Mensagens, eventos e comandos
• Queue-based load leveling
• Comunicação baseada em eventos
• Request-reply assíncrono

**Desenhar um message broker no Azure**

• Particionamento
• Push vs. pull
• Mecanismos pub-sub

• O padrão claim-check
• Recursos do Azure: Service Bus, Event Grid e Storage Queues

**Consistência de dados**

• Consistência forte
• O teorema CAP
• Consistência eventual
• O padrão outbox
• O padrão compensating transaction
• LAB: implementar consistência eventual

**CQRS e Event Sourcing**

• O problema do CRUD
• Modelos de leitura e de escrita
• Comandos
• Event store
• LAB: implementar um carrinho de compras com CQRS

**Comunicação externa**

• API gateway
• Backend for frontends
• Request-reply assíncrono
• Webhooks
• Recursos do Azure: API Management, Front Door e Logic Apps
• LAB: aceder a exames médicos com Logic Apps

**Questões de segurança**

• Opções para guardar dados sensíveis
• Azure Key Vault e managed identity
• Autenticação de serviços
• Segurança ao nível da infraestrutura: redes virtuais, firewalls, ...
• O padrão gatekeeper