MBA USP ESALQ

Infra As Code (IAC)

Wesley Milan

*A responsabilidade pela idoneidade, originalidade e licitude dos conteúdos didáticos apresentados é do professor.

Quem é Wesley Milan?

- Programador há mais de 36 anos
- AWS há mais de 14 anos
- Especialista em:
    - Segurança de aplicações
    - Plataformas de alta demanda
    - Otimização de custos
    - Gestão de alta performance
- +70 projetos de sistemas web e off-line
- Áreas de e-commerce, saúde, engenharia, financeira, turismo, alimentícia entre outras.
- Projeto Grand Canion/US: Mais de 40 mil usuários simultâneos, ataque DDoS com mais de 30 mil bots, faturamento de mais de U$18M em 40 minutos.
- Programador, DBA, arquiteto de soluções, líder técnico, diretor, CTO, empreendedor, professor, inventor e mesmo assim, um eterno aprendiz.

Evolução da infraestrutura

Uma breve história sobre infraestrutura em nuvem

Para aprender a usar é necessário saber como a ferramenta funciona, e para saber como ela funciona é necessário saber como ela foi construída.

Uma breve história sobre infraestrutura em nuvem

Anos 90:

- Servidores eram implantados dentro dos provedores de acesso à internet.
- Os servidores eram computadores comuns que não tinham mais potência para serem usados como desktops.
- Pagávamos pelo serviço e não pela solução.
- Não havia redundância de energia.
- Não havia redundância de link.
- Não havia redundância de dados.
- Não havia segurança de infraestrutura.
- E toda interação com o hardware era feita através de A.P.I. (Alguém que Pressiona o Interruptor).

Uma breve história sobre infraestrutura em nuvem

Anos 2000:

- Serviços como CPanel começam a ganhar mercado.
- Processadores multi-core se tornam mais populares.
- OS links ficam mais poderosos.
- Data centers de hospedagem mais bem estruturados surgem.
- Os serviços de hospedagem evoluem para ambientes compartilhados dentro de hardwares mais fortes.
- A interação com o hardware ainda é por A.P.I. (Alguém que Pressiona o Interruptor).
- Ganha-se uma vantagem com máquinas virtualizadas, o reboot remoto do ambiente virtual.
- É o começo de uma versão tímida do que viria a ser Infra As Code.

Uma breve história sobre infraestrutura em nuvem

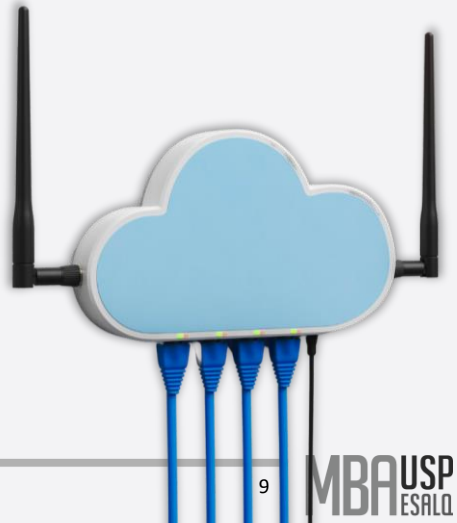
De 2003 a 2006:

- A Amazon (e-commerce) precisa de soluções que não existem no mercado
  - Alta escalabilidade para suportar picos de tráfego
  - Elasticidade para reduzir o custo operacional quando não tiver demanda
  - Flexibilidade para diferentes tipos de projetos
  - Extensibilidade para derivar serviços a partir de outros serviços
  - Redundância de dados, energia e link
  - Segurança
- Surge o S3
- Surge o SQS
- Surge o EC2
- Surgem diversos outros serviços derivados como SNS, RDS, etc.

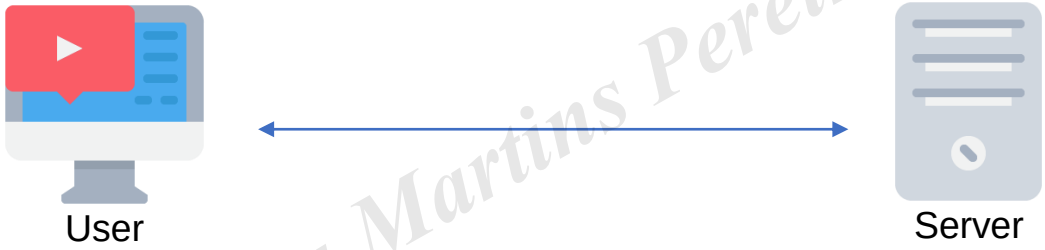
Uma breve história sobre infraestrutura em nuvem

Diferenciais do hardware em nuvem

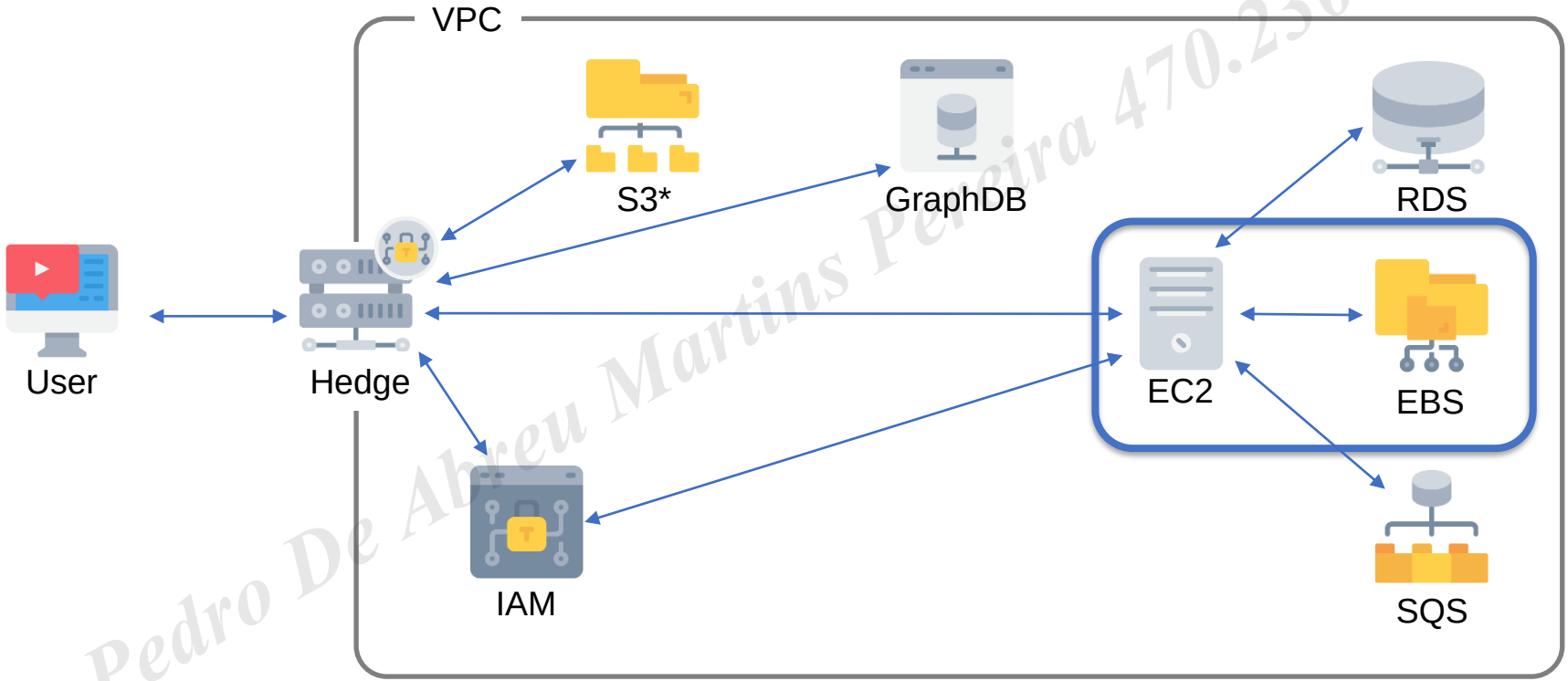
- Hardware compartilhados com alto controle sobre o consumo
- Redundância
  - Múltiplas placas de rede
  - Múltiplos links
  - Múltiplas fontes de alimentação
  - Múltiplas redes elétricas com alimentação de emergência
- Segurança física e lógica
- Controle e monitoramento remoto do hardware em nível granular



Arquitetura Client/Server

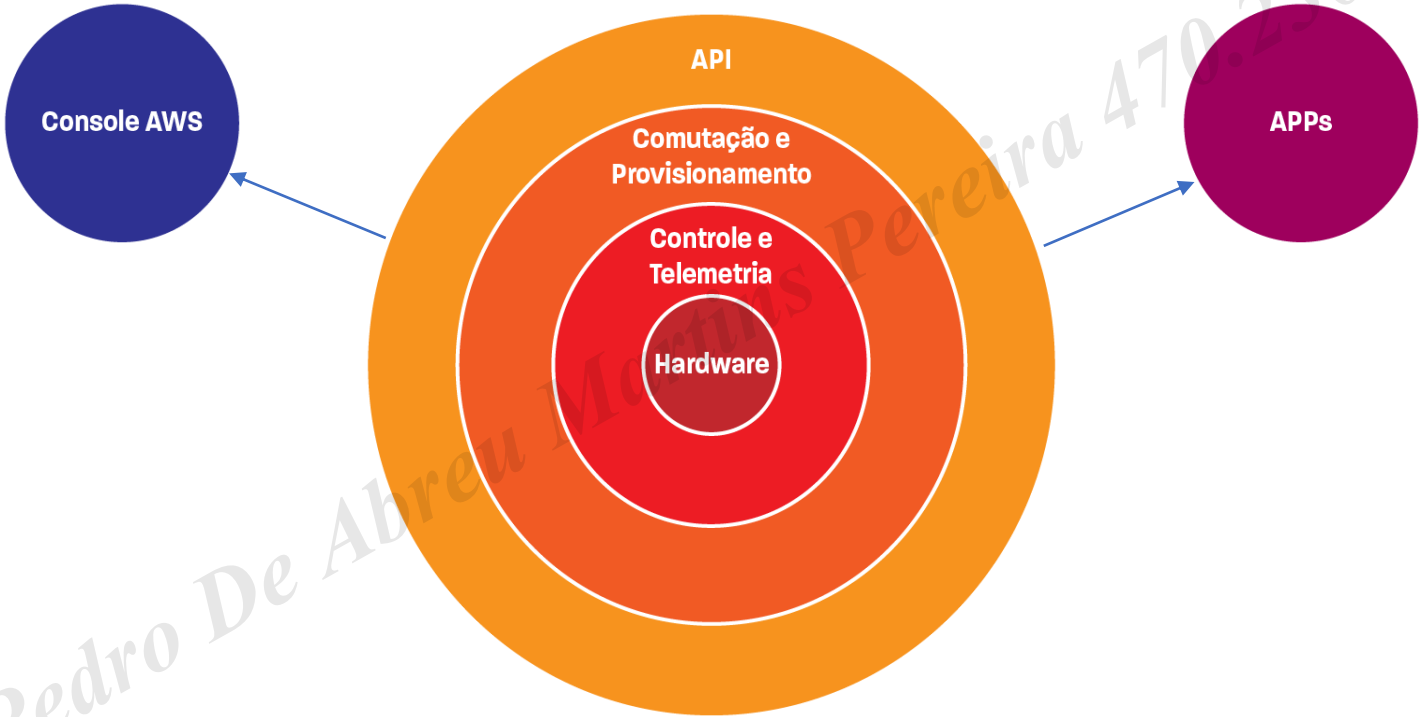


Arquitetura Cloud (conceito fundamental)



* Serviços independentes não estão submissos à uma VPC, mas respondem igualmente à autoridade do IAM e aos serviços de borda

Onion Architectural Vision



Provedores

Provedores Cloud

Serviços de Integração

HashiCorp Terraform

Infrastructure as code
Use infrastructure as code to automate the provisioning of your infrastructure including servers, databases, firewall policies, and almost any other resource.

Multi-cloud provisioning
Deploy serverless functions with AWS Lambda, manage Microsoft Azure Active Directory resources, provision a load balancer in Google Cloud, and more.

Manage Kubernetes
Provision and manage Kubernetes clusters on AWS, Microsoft Azure, or Google Cloud, and interact with your cluster using the Kubernetes Terraform provider.

Manage network infrastructure
Automate key networking tasks like updating load balancer target pools or applying firewall policies.

Manage virtual images
Build and manage virtual images with Terraform and Packer.

Integrate with existing workflows
Automate infrastructure deployments through existing CI/CD workflows.

Enforce policy as code
Enforce policy guardrails before your users create infrastructure using Sentinel policy as code.

Inject secrets into Terraform
Use HashiCorp Vault to automate the usage of dynamically generated secrets and credentials within Terraform configurations.

amazon web services

Google Cloud

Azure

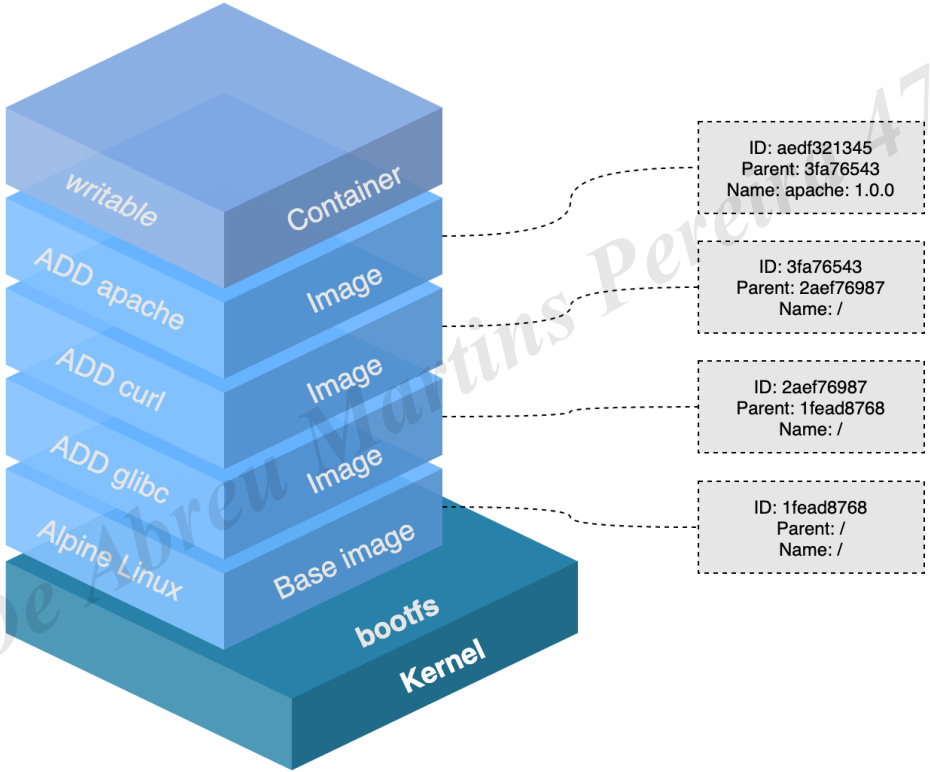
ORACLE CLOUD

Fonte: https://www.terraform.io/

Serviços de Integração

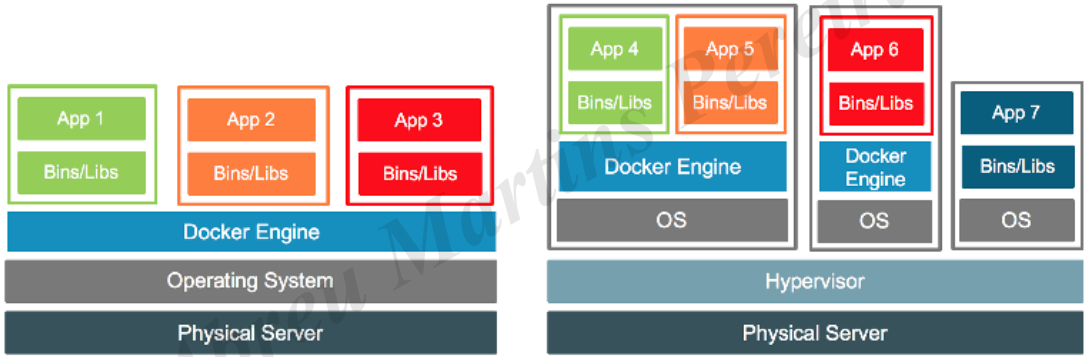
kubernetes

Serviços de Integração



Fonte: https://ragin.medium.com/docker-what-it-is-how-images-are-structured-docker-vs-vm-and-some-tips-part-1-d9686303590f

Serviços de Integração



Fonte: https://www.sweharris.org/post/2017-06-18-buildcontainer/

Perguntas e Intervalo

Isolamento

Isolamento Físico

- Restrições vantajosas:
  - Não é necessário que operadores estejam presencialmente no data center.
  - Não é necessário que operadores acessem fisicamente os servidores.
- Ganhos de Produtividade:
  - Monitoramento remoto de cada elemento do ecossistema.
  - Monitoramento automatizado.
  - Análise de telemetria e desempenho do hardware.
  - Migração remota de recursos lógicos.
  - Identificação automatizada de degradação ou falhas de hardware.
  - Manutenção programada.
- Melhoria de segurança:
  - Acesso reduzido ao hardware.
  - Redução de chances de vazamento ou comprometimento de dados.
  - Redução ocorrências de acidentes e erros humanos.
  - Controle de danos e compartimentação de efeitos colaterais.
- Ganhos financeiros:
  - Aumento da capacidade de escala de gestão dos recursos tecnológicos.
  - Redução de incidentes.
  - Redução de consumo de recursos energéticos.
  - Preços mais competitivos e flexíveis.

Isolamento Lógico

- Estabilidade:
  - Redundância de recursos.
  - Redução de pontos de falha.
  - Balanceamento de recursos.
  - Migração de recursos e aplicações sem interferência dos operadores do data center.
- Produtividade:
  - Independência no controle da infraestrutura.
  - Integração via código ou ferramentas de terceiros para gestão automatizada.
  - Acesso às métricas de infraestrutura e aplicações para análise e otimização.
  - Abstração de infraestrutura para consumo e desenvolvimento de serviços.
  - Versionamento e controle de ambientes.
- Segurança:
  - Dados transitórios criptografados.
  - Dados estacionários criptografados.
  - Alta granularidade nos níveis de permissões.
  - Alta granularidade de rede em nível lógico.
- Controle:
  - Autonomia de segurança.
  - Autonomia de provisionamento.
  - Autonomia de escalabilidade.
  - Autonomia de controle de acesso.
- Custos:
  - Consumo de recursos controlado pelo cliente em tempo real.
  - Automação.
  - Integração.
  - Controle aberto e transparente dos custos.

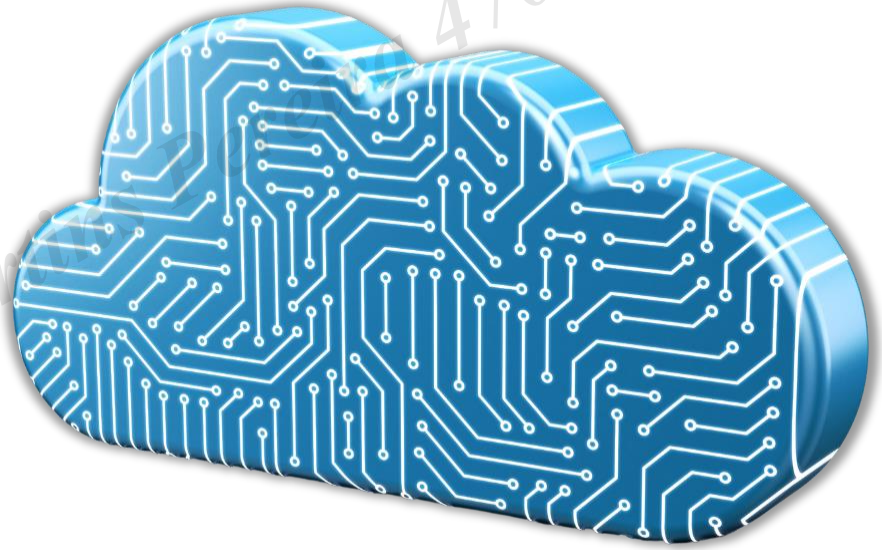
Inovação

- Acesso a hardware e software de última geração sem imobilizar patrimônio.
- Integração de APIs de terceiros que utilizam sua própria conta para executar aplicações e serviços de última geração.
- A facilidade de qualquer um se tornar um provedor de serviços especializados.
- A granularidade permite criar, validar e, evoluir ou encerrar projetos com rapidez e baixos custos.
- Consumir serviços e softwares sob demanda sem a necessidade de aquisição de licenças e sem carência de uso.

Granularidade

Fundamentos de Infraestrutura Cloud

- Categorias de serviços AWS
  - Análises
  - Integração de aplicações
  - Blockchain
  - Aplicações empresariais
  - Gerenciamento financeiro na nuvem
  - Computação
  - Central de atendimento
  - Contêineres
  - Banco de dados
  - Ferramentas de desenvolvedor
  - Computação de usuário final
  - Web e plataforma móvel front-end
  - Jogos
  - Internet das Coisas
  - Machine learning
  - Gerenciamento e governança
  - Serviços de mídia
  - Migração e transferência
  - Redes e entrega de conteúdo
  - Tecnologias quânticas
  - Robótica
  - Satélite
  - Segurança, identidade e conformidade
  - Tecnologia sem servidor
  - Armazenamento
  - Cadeia de suprimentos

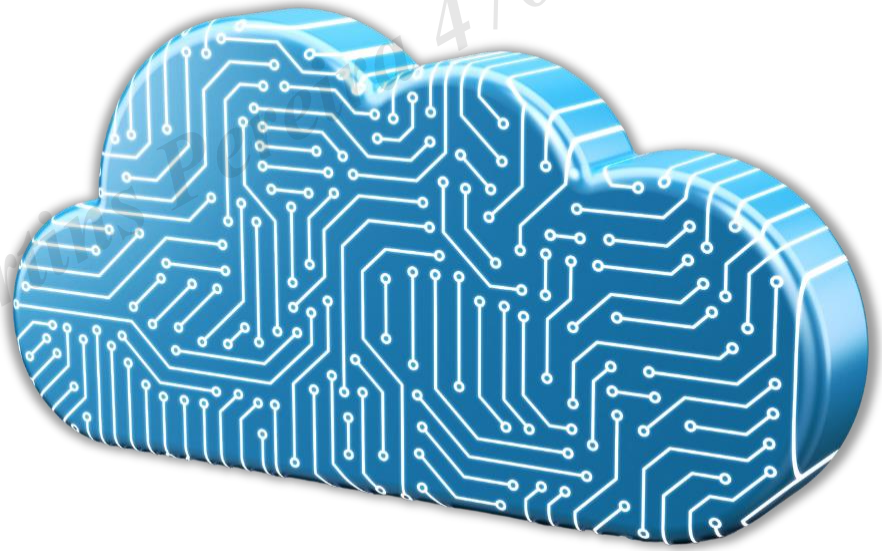


Fundamentos de Infraestrutura Cloud

1. Amazon Athena
2. Amazon CloudSearch
3. Amazon DataZone
4. Amazon OpenSearch Service
5. Amazon EMR
6. Amazon FinSpace
7. Amazon Kinesis
8. Amazon Managed Service for Apache Flink
9. Amazon Managed Streaming for Apache Kafka
10. Amazon Redshift
11. Amazon QuickSight
12. AWS Clean Rooms
13. AWS Data Exchange
14. AWS Data Pipeline
15. AWS Entity Resolution
16. AWS Glue
17. AWS Lake Formation
18. AWS Step Functions
19. Amazon AppFlow
20. Amazon EventBridge
21. Amazon Managed Workflows for Apache Airflow
22. Amazon MQ
23. Amazon Simple Notification Service (SNS)
24. Amazon Simple Queue Service (SQS)
25. AWS AppSync
26. B2B Data Interchange
27. Amazon Managed Blockchain
28. Amazon Quantum Ledger Database (QLDB)
29. AWS AppFabric
30. Amazon Connect
31. Carrinho do Amazon Dash
32. Amazon One
33. Amazon One Enterprise (prévia)
34. Amazon Pinpoint
35. Cadeia de Suprimentos AWS
36. Tecnologia Just Walk Out
37. Amazon Chime
38. AWS Wickr
39. Amazon WorkDocs
40. Amazon WorkMail
41. Alexa for Business
42. Amazon Chime SDK
43. Amazon Simple Email Service (SES)
44. APIs do Amazon Pinpoint
45. Amazon Chime Voice Connector
46. Amazon WorkDocs SDK
47. Explorador de Custos da AWS
48. AWS Billing Conductor
49. AWS Budgets
50. AWS Cost and Usage Report
51. Relatórios de instâncias reservadas
52. Savings Plans
53. Amazon EC2
54. Amazon EC2 Auto Scaling
55. Amazon Lightsail
56. AWS App Runner
57. AWS Batch
58. AWS Elastic Beanstalk
59. AWS Lambda
60. Zonas locais da AWS
61. AWS Outposts
62. AWS Serverless Application Repository
63. AWS SimSpace Weaver
64. Família AWS Snow
65. AWS Wavelength
66. VMware Cloud on AWS
67. Amazon Elastic Container Registry
68. Amazon Elastic Container Service (ECS)
69. Amazon ECS Anywhere
70. Amazon Elastic Kubernetes Service (EKS)
71. Amazon EKS Anywhere
72. Amazon EKS Distro
73. AWS App2Container
74. AWS Copilot
75. AWS Fargate
76. Red Hat OpenShift Service on AWS
77. Amazon Aurora
78. Amazon Aurora Sem Servidor v2
79. Amazon DocumentDB (compatível com MongoDB)
80. Amazon DynamoDB
81. Amazon ElastiCache
82. Amazon Keyspaces (for Apache Cassandra)
83. Amazon MemoryDB for Redis
84. Amazon Neptune
85. Amazon RDS
86. Amazon RDS on Outposts
87. Amazon Timestream
88. AWS Database Migration Service
89. Amazon CodeCatalyst
90. Amazon CodeGuru
91. Amazon Corretto
92. Amazon CodeWhisperer
93. API de Controle da Nuvem AWS
94. AWS Cloud Development Kit (CDK)
95. AWS Cloud9
96. AWS CloudShell
97. AWS CodeArtifact
98. AWS CodeBuild
99. AWS CodeCommit
100. AWS CodeDeploy
101. AWS CodePipeline
102. AWS CodeStar
103. Interface da linha de comando da AWS
104. AWS Device Farm
105. AWS Fault Injection Service
106. AWS Serverless Application Model
107. Ferramentas e SDKs da AWS
108. AWS X-Ray
109. Thin client do Amazon WorkSpaces
110. Amazon AppStream 2.0
111. AWS Amplify
112. Amazon API Gateway
113. Amazon Location Service
114. Amazon GameLift
115. Amazon GameSparks
116. Amazon Lumberyard
117. AWS GameKit
118. AWS IoT 1-Click
119. AWS IoT Analytics
120. AWS IoT Button
121. AWS IoT Core
122. AWS IoT Device Defender
123. AWS IoT Device Management
124. AWS IoT Events
125. AWS IoT ExpressLink
126. AWS IoT FleetWise
127. AWS IoT Greengrass
128. AWS IoT RoboRunner
129. AWS IoT SiteWise
130. AWS IoT TwinMaker
131. AWS Partner Device Catalog
132. Amazon Kinesis Video Streams
133. FreeRTOS
134. Amazon Bedrock
135. Amazon SageMaker
136. Amazon Augmented AI
137. Amazon Comprehend
138. Amazon Comprehend Medical
139. Amazon DevOps Guru
140. Amazon Elastic Inference
141. Amazon Forecast
142. Amazon Fraud Detector
143. Amazon Kendra
144. Amazon Lex
145. Amazon Lookout for Equipment
146. Amazon Lookout for Metrics
147. Amazon Lookout for Vision
148. Amazon Monitron
149. AWS HealthOmics
150. AWS HealthImaging
151. AWS HealthScribe
152. AWS HealthLake
153. Amazon Personalize
154. Amazon Polly
155. Amazon Rekognition
156. Amazon Textract
157. Amazon Translate
158. Amazon Transcribe
159. Amazon Q (prévia)
160. AMIs do AWS Deep Learning
161. AWS Deep Learning Containers
162. AWS DeepComposer
163. AWS DeepLens
164. AWS DeepRacer
165. AWS Inferentia
166. AWS Panorama
167. Apache MXNet on AWS
168. PyTorch na AWS
169. TensorFlow na AWS
170. Amazon CloudWatch
171. Amazon Managed Grafana
172. Amazon Managed Service for Prometheus
173. AWS Auto Scaling
174. AWS Chatbot
175. AWS CloudFormation
176. AWS CloudTrail
177. AWS Compute Optimizer
178. AWS Config
179. AWS Control Tower
180. Aplicativo móvel do Console AWS
181. AWS Distro para OpenTelemetry
182. AWS Health Dashboard
183. AWS Launch Wizard
184. AWS License Manager
185. Console de Gerenciamento da AWS
186. AWS Managed Services
187. AWS OpsWorks
188. AWS Organizations
189. AWS Proton
190. AWS Resilience Hub
191. AWS Service Catalog
192. AWS Service Management Connector
193. AWS Systems Manager
194. AWS Telco Network Builder
195. AWS Trusted Advisor
196. AWS Well-Architected Tool
197. Amazon Elastic Transcoder
198. Serviço de vídeo interativo da Amazon
199. Amazon Nimble Studio
200. AWS Elemental MediaConnect
201. AWS Elemental MediaConvert
202. AWS Elemental MediaLive
203. AWS Elemental MediaPackage
204. AWS Elemental MediaStore
205. AWS Elemental MediaTailor
206. Dispositivos e software do AWS Elemental
207. AWS Thinkbox Deadline
208. AWS Thinkbox Frost
209. AWS Thinkbox Krakatoa
210. AWS Thinkbox Sequoia
211. AWS Thinkbox Stoke
212. AWS Thinkbox XMesh
213. AWS Migration Hub
214. AWS Application Discovery Service
215. AWS Application Migration Service (MGN)
216. AWS DataSync
217. AWS Mainframe Modernization
218. AWS Snow Family
219. AWS Transfer Family
220. Migration Evaluator (o antigo TSO Logic)
221. Amazon VPC
222. Amazon VPC Lattice
223. Amazon CloudFront
224. Amazon Route 53
225. AWS App Mesh
226. AWS Cloud Map
227. AWS Cloud WAN
228. AWS Direct Connect
229. AWS Global Accelerator
230. AWS Private 5G
231. AWS PrivateLink
232. AWS Transit Gateway
233. Acesso Verificado pela AWS
234. AWS VPN
235. Elastic Load Balancing (ELB)
236. Amazon Braket
237. Amazon Quantum Solutions Lab
238. AWS RoboMaker
239. AWS Ground Station
240. AWS Identity and Access Management (IAM)
241. Amazon Cognito
242. Amazon Detective
243. Amazon GuardDuty
244. Amazon Inspector
245. Amazon Macie
246. Amazon Security Lake
247. Amazon Verified Permissions
248. AWS Artifact
249. AWS Audit Manager
250. AWS Certificate Manager
251. AWS CloudHSM
252. AWS Directory Service
253. AWS Firewall Manager
254. AWS Key Management Service
255. AWS Network Firewall
256. AWS Payment Cryptography
257. AWS Private Certificate Authority
258. AWS Resource Access Manager
259. AWS Secrets Manager
260. AWS Security Hub
261. AWS Shield
262. Centro de Identidade do AWS IAM
263. AWS WAF
264. Amazon Simple Storage Service (S3)
265. AWS Application Composer
266. Classes de armazenamento Amazon S3 Glacier
267. Amazon Elastic Block Store (EBS)
268. Amazon Elastic File System (EFS)
269. Amazon FSx for Lustre
270. Amazon FSx for NetApp ONTAP
271. Amazon FSx for OpenZFS
272. Amazon FSx for Windows File Server
273. Amazon File Cache
274. AWS Backup
275. AWS Elastic Disaster Recovery (DRS)
276. AWS Storage Gateway

Fundamentos de Infraestrutura Cloud

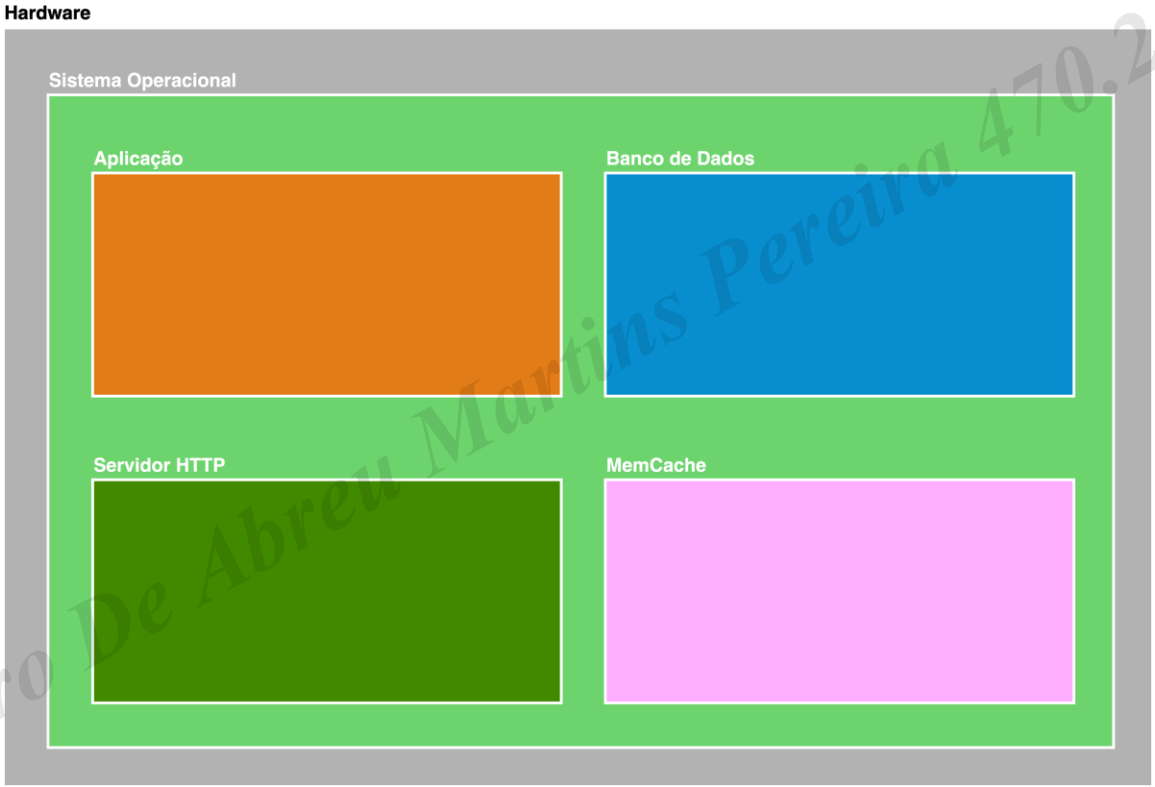
- Macro categorias de serviços em nuvem
  - Computacionais
    - EC2
    - Lambda
    - Machine Learning
    - ...
  - Dados
    - S3
    - RDS
    - ...
  - Rede
    - VPC
    - VPN
    - ...
  - Borda
    - Firewall
    - WAF
    - CloudFront
    - ELB
    - ...



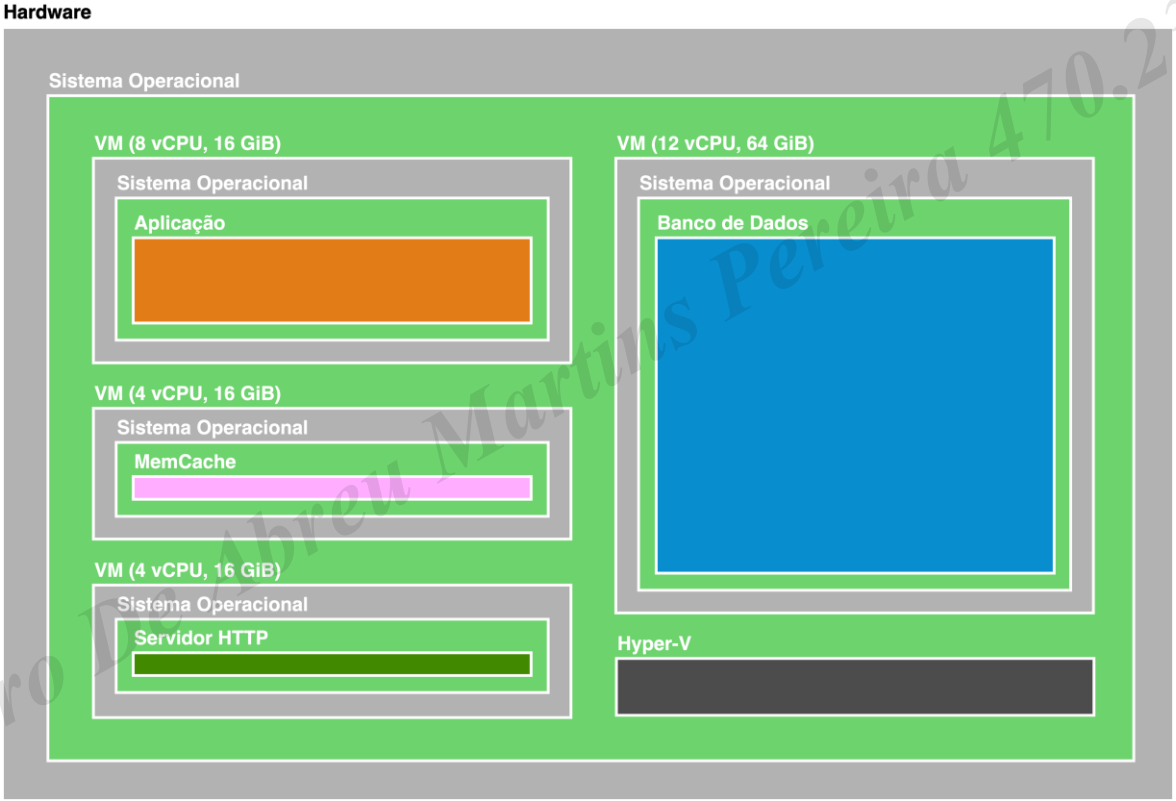
Fundamentos de Infraestrutura Cloud

- Abstração de serviços
  - Quanto mais próximo da computação pura mais barato é o custo computacional CPU/Memória.
  - Quanto mais abstraído maior é o custo/tempo.
  - Quanto mais abstraído mais especializado.
  - Processos de consumo constante custam mais barato em serviços computacionais como EC2.
  - Processos de consumo esporádico e oscilante custam mais barato em serviços elásticos com Lambda, Fargate, Kubernetes e similares. O mesmo vale para bancos de dados.
  - Use a granularidade da nuvem a seu favor para ganhar escalabilidade a custos baixos.

Otimização de recursos computacionais



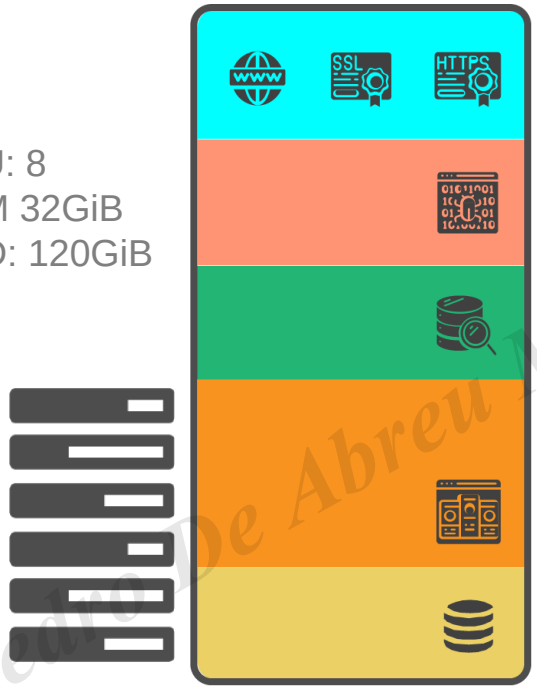
Otimização de recursos computacionais



Otimização de recursos computacionais

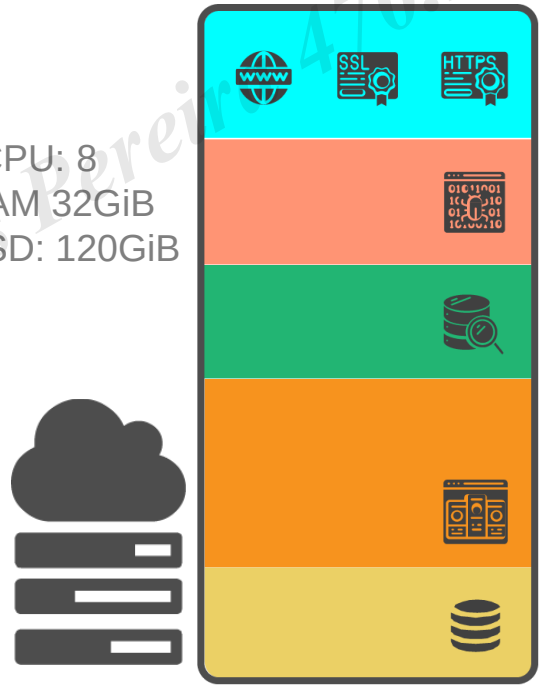
OnPremises / Dedicado

CPU: 8
RAM 32GiB
HDD: 120GiB



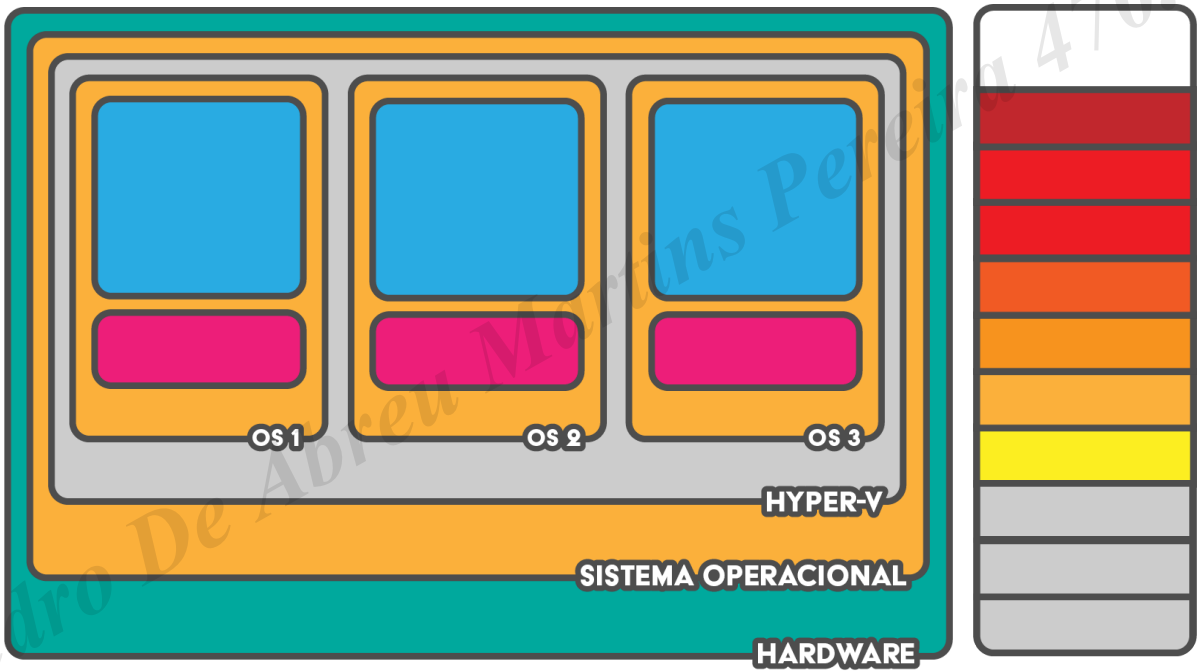
Instância Cloud

vCPU: 8
RAM 32GiB
SSD: 120GiB



Otimização de recursos computacionais

Instância Virtualizada em Cloud



Otimização de recursos computacionais

Logs / Monitoramento

OpenSearch Service

CloudWatch

Search Engine

CloudSearch

Banco de Dados

Aurora/RDS

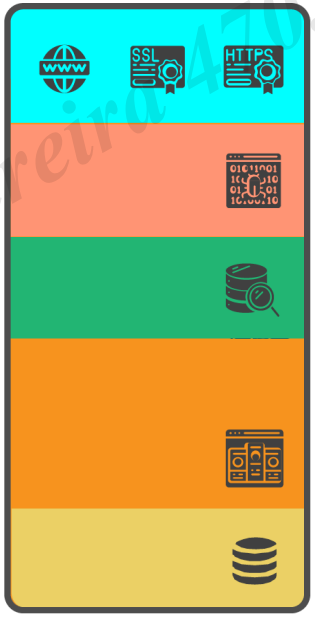
Utilitários

Route 53

Elastic Load Balancing

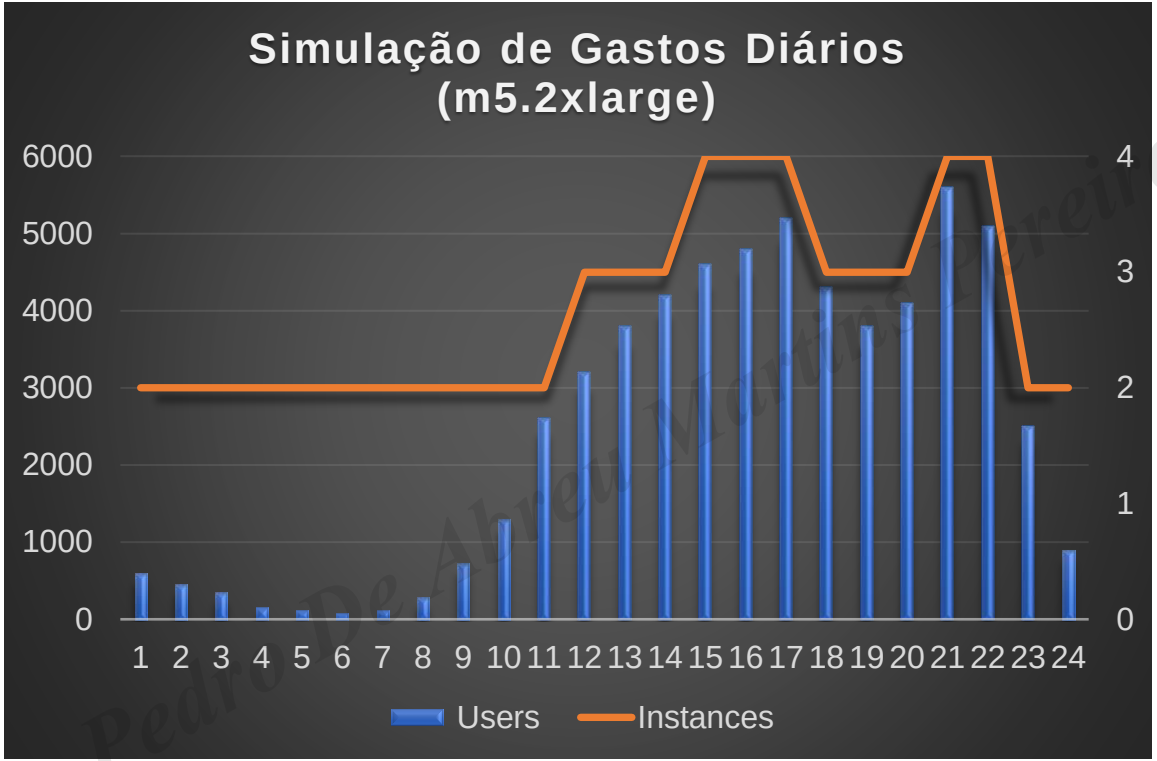
AWS Certificate Manager (ACM)

Instância Cloud



vCPU: 8
RAM 32GiB
SSD: 120GiB

Otimização de recursos computacionais



Instância

Instância: m5.2xlarge
vCPU: 8
RAM: 32GiB
U$/h: 0,384
U$/m: 280,32

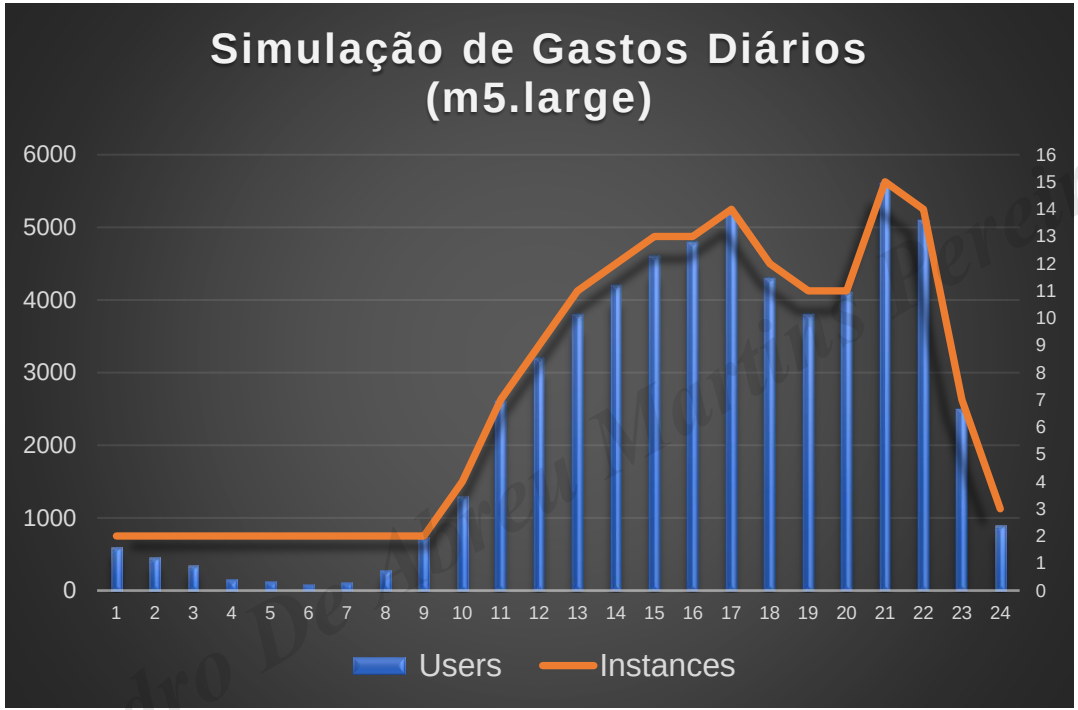
Cenário

Requisições: 50 r/s
Req/Min: 2
Usua. Sim.: 1.500
Méd. CPU: 60%
CPU / Usua.: 0,04%

Custos

Horas/Dia/Inst.: 64
U$/d: 24,58
U$/m: 737,28

Otimização de recursos computacionais



Instância

Instância: m5.large
vCPU: 2
RAM: 8GiB
U$/h: 0,096
U$/m: 70,08

Cenário

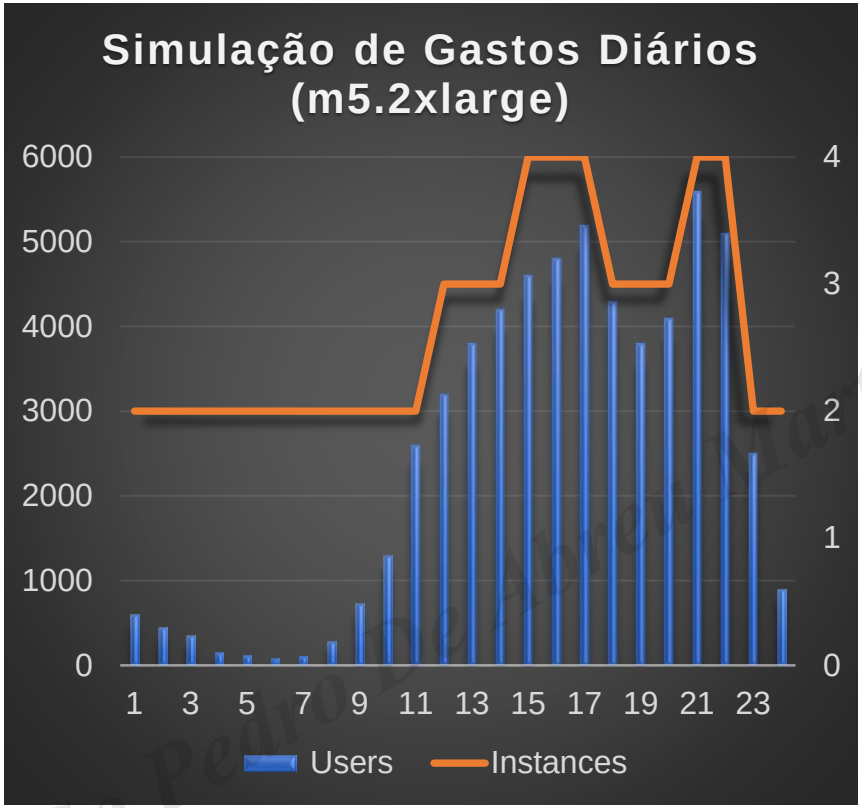
Requisições: 12,5 r/s
Req/Min: 2
Usua. Sim.: 375
Méd. CPU: 60%
CPU / Usua.: 0,04%

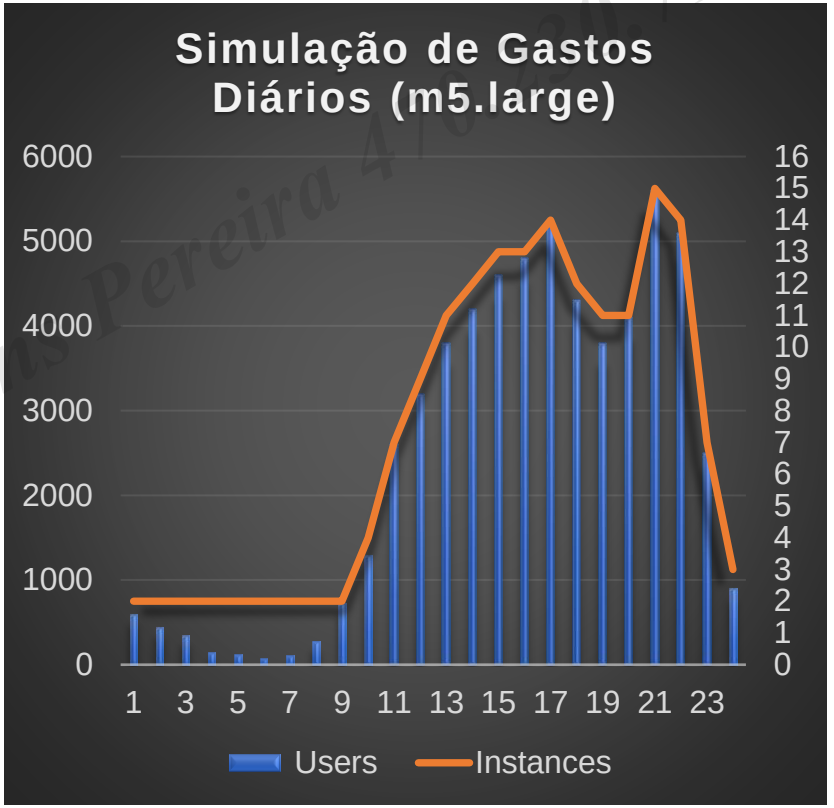
Custos

Horas/Dia/Inst.: 174
U$/d: 16,70
U$/m: 501,12

U$/m: 737,28
Econ.: 32%

Otimização de recursos computacionais





Granularidade

- Instâncias menores
- Auto escalabilidade
- Ambientes enxutos
- Microsserviços
- Serviços distribuídos
- Gestão de dados independente

R: Automação

Perguntas e Intervalo

Arquitetura

Estrutura de Projetos com IaC

Well Architected Frameworks
Princípios:

- Pare de adivinhar suas necessidades de capacidade
- Sistemas de teste em escala de produção
- Automatize tendo em mente a experimentação arquitetônica
- Considere arquiteturas evolucionárias
- Impulsione arquiteturas usando dados
- Melhore durante os dias de jogo

Referências:

- AWS: https://aws.amazon.com/architecture/well-architected
- Azure: https://learn.microsoft.com/en-us/azure/well-architected/
- Google: https://cloud.google.com/architecture/framework

Estrutura de Projetos com IaC

Well Architected Frameworks
Pilares:

- Excelência operacional
- Segurança
- Confiabilidade
- Eficiência de desempenho
- Otimização de custos
- Sustentabilidade

Referências:

- AWS: https://aws.amazon.com/architecture/well-architected
- Azure: https://learn.microsoft.com/en-us/azure/well-architected/
- Google: https://cloud.google.com/architecture/framework

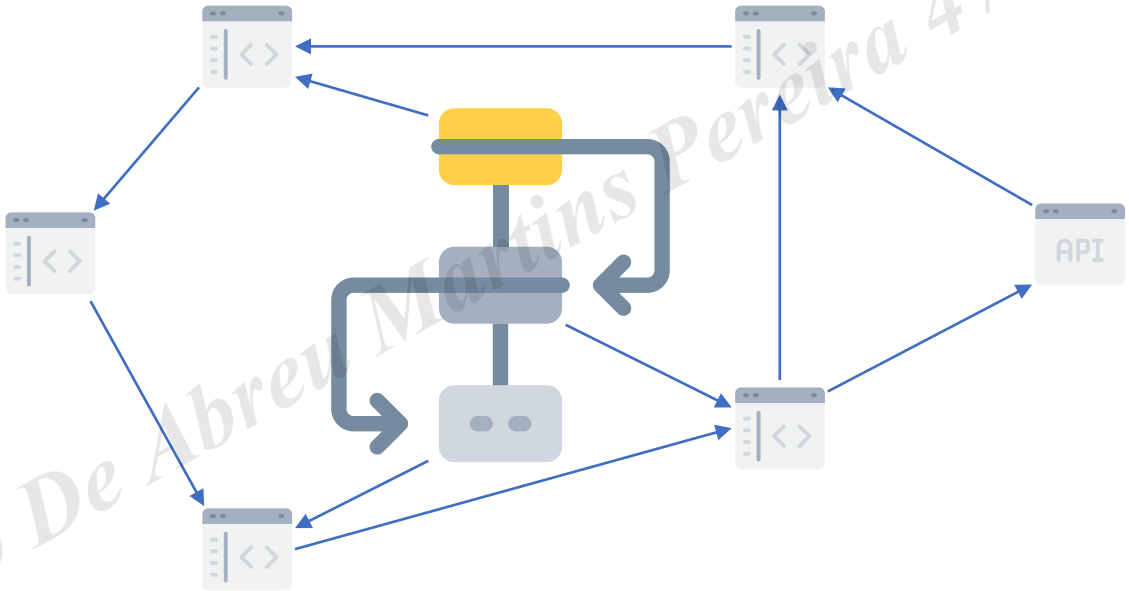
Estrutura de Projetos com IaC

Princípios da arquitetura eficiente

- Acoplamento fraco
- Gestão de dados independente
- Independência de camadas
- Versionamento
- Testes
- Automação de deploys / pipelines
- Monitoramento
- Plano de contingência
- Autorreparação
- Análise e evolução constante

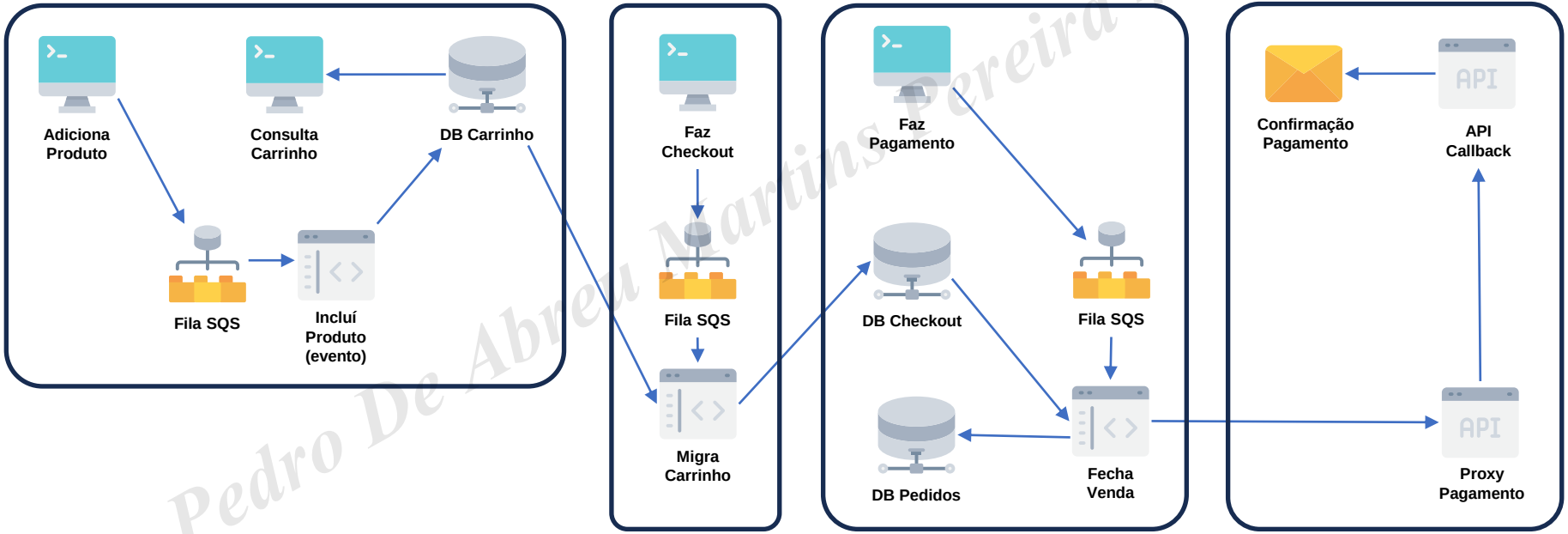
Estrutura de Projetos com IaC

Acoplamento forte



Estrutura de Projetos com IaC

Acoplamento fraco com assincronicidade (carrinho de compras)



Estrutura de Projetos com IaC

Gestão de dados independente (NoSQL)

- Schemeless
- Alta performance
- Gestão compartilhada entre memória e disco
- *Persistência eventual
- Big Data
- Redundância / Cluster
- Backup difícil

Estrutura de Projetos com IaC

Gestão de dados independente (Key/Value)

- Chave/Valor
- Alta performance
- Gestão compartilhada entre memória e disco
- *Persistência eventual e volátil
- Alto custo de escala
- Alto custo de armazenamento
- Redundância / Cluster
- Sem Backup

Estrutura de Projetos com IaC

Gestão de dados independente (Objetos)

- Schemeless
- *Performance média
- *Persistência forte
- Baixo custo de escala
- Baixo custo de armazenamento
- *Alto custo de recuperação de dados
- Redundância
- Backup / Replicação

Estrutura de Projetos com IaC

Gestão de dados independente (SQL)

- Schema
- *Performance baixa
- *Persistência forte
- Alto custo de escala
- Alto custo de armazenamento
- *Redundância e Cluster de alta complexidade
- Backup / Replicação

Perguntas
E
Intervalo

OBRIGADO!

www.linkedin.com/in/wesleymilan/?_l=pt_BR