

20 - Analisando Riscos de Arquitetura

2025-12-23 16:07 pm

Lidar com os riscos dos problemas de cada arquitetura.

Matriz de Risco

- Classificar o risco entre alto, médio e baixo.
- Impacto X Probabilidade.

		Likelihood of risk occurring		
		Low (1)	Medium (2)	High (3)
Overall impact of risk	Low (1)	1	2	3
	Medium (2)	2	4	6
	High (3)	3	6	9

- *Figure 20-1. Matrix for determining architecture risk*

Avaliação de Risco

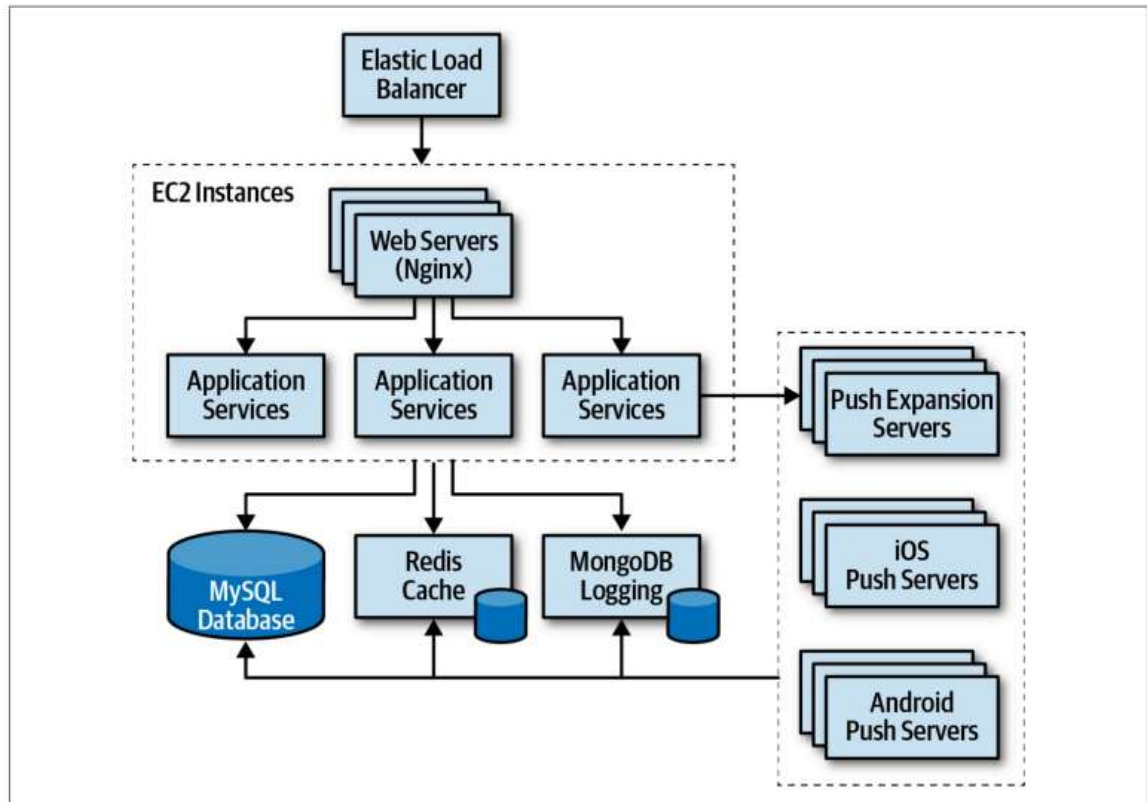
- Risco por critério para cada domínio.

RISK CRITERIA	Customer registration	Catalog checkout	Order fulfillment	Order shipment	TOTAL RISK
Scalability	2	6	1	2	11
Availability	3	4	2	1	10
Performance	4	2	3	6	15
Security	6	3	1	1	11
Data integrity	9	6	1	1	17
TOTAL RISK	24	21	8	11	

- *Figure 20-2. Example of a standard risk assessment*
- Verifica-se o risco total de cada critério ou de cada domínio.
- Pode ser conveniente mostrar apenas os campos de alto risco numa apresentação.
 - Exclui todos os valores que não são 6 e 9 e a matriz é refeita, com o resto em branco.
- Não diz se está melhorando ou piorando com o tempo.
 - Podemos colocar ao lado de cada número um +/- ou um a seta indicando se subiu ou diminuiu do valor anterior.
- Funções de score podem definir o valor do risco objetivamente, se for possível.

Risk Storming

- Risco do sistema não pode ser determinado apenas pelo arquiteto sozinho.
 - Ignora ou desconhece alguns aspectos do sistema.
- Risk Storming é o exercício colaborativo de considerar riscos com outros arquitetos e desenvolvedores também.
 - Primeiro individualmente e depois em grupo.
- Três atividades:
 1. Identificação
 2. Consenso
 3. Mitigação
- Arquitetura exemplo:



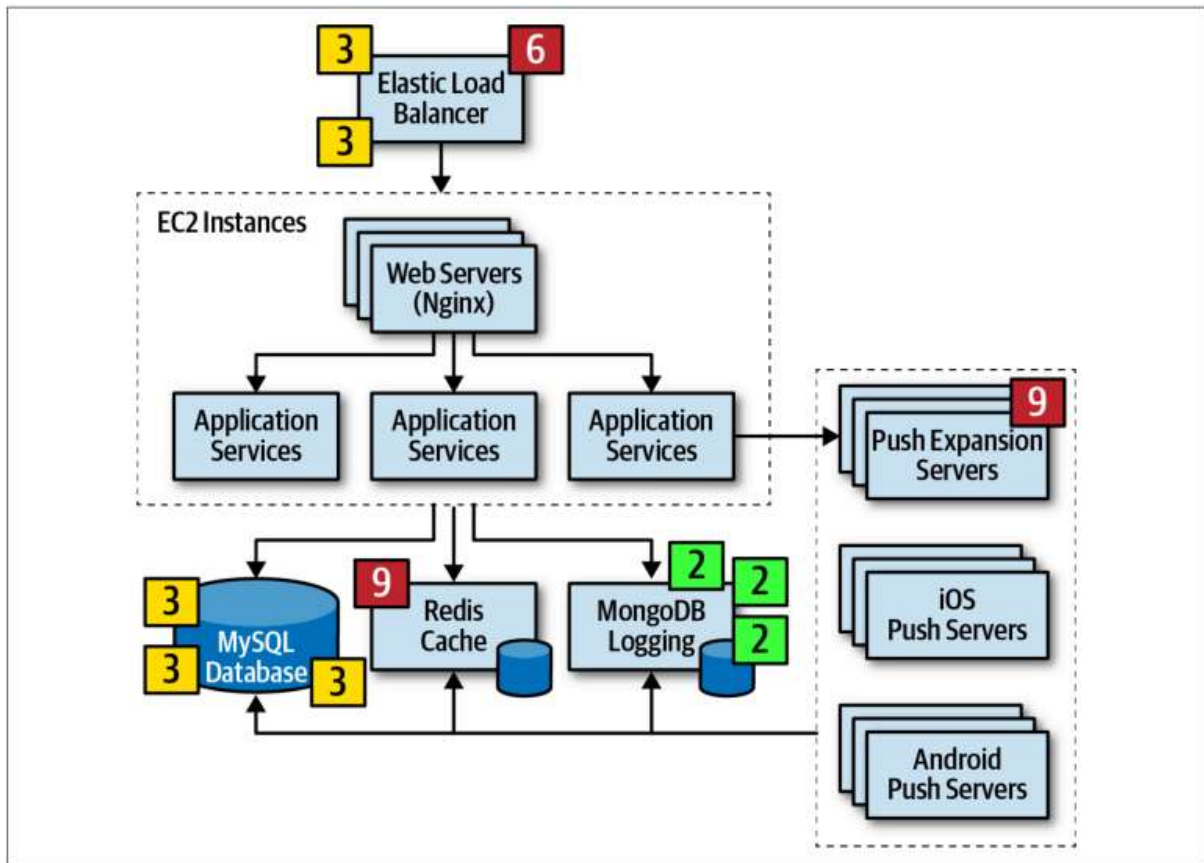
○ *Figure 20-6. Architecture diagram for risk storming example*

Identificação

- Cada participante descreve uma área de risco da arquitetura.
- Primeiro cada participante preenche a matriz de risco sozinho.
- Cada sessão de Risk Storming deve discutir um único critério (e.g. Desempenho), de preferência.

Consenso

- Etapa de discutir coletivamente
- É bom ter o diagrama da arquitetura desenhado bem grande em algum lugar.
- Participantes colocam post-its indicando nível de risco em cada lugar do diagrama.



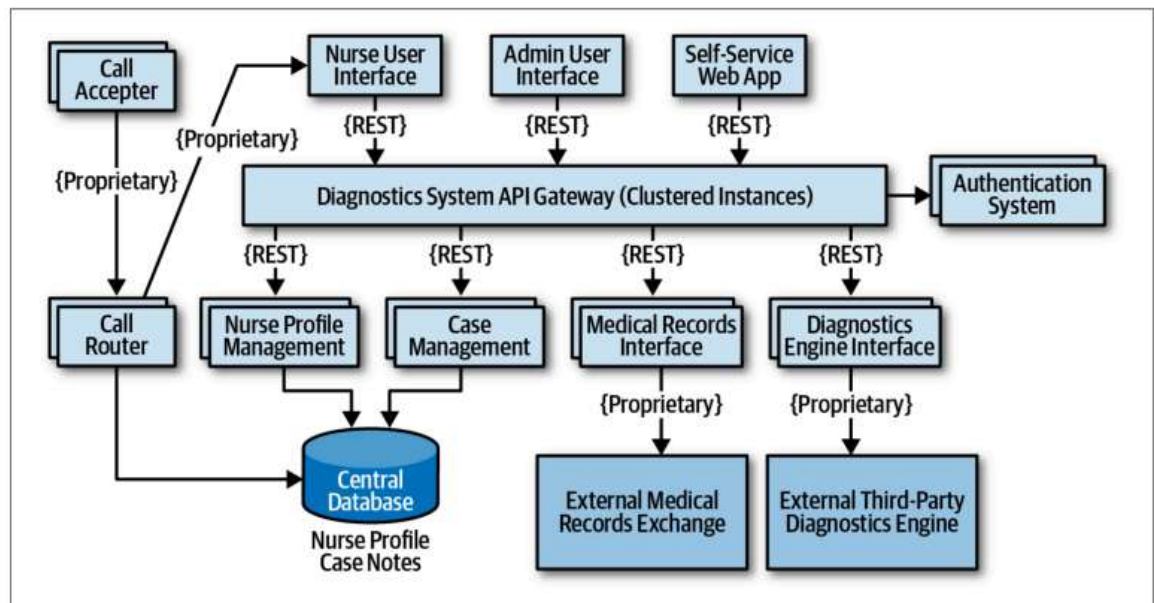
- *Figure 20-7. Initial identification of risk areas*
- Objetivo desta etapa é gerar um consenso.
- Onde já houve consenso inicial não há por que haver discussão mais neste momento.
- Cada participante argumenta em favor de sua avaliação.
- Para tecnologia desconhecidas ou não-testadas, sempre associar nota máxima (9) de risco.
- Discussão é feita até que reste só um post-it em cada área de risco que deva existir.

Mitigação

- Discutir mudanças e melhorias no sistema para minimizar riscos.
- Etapa requer um stakeholder para dizer qual custo faz sentido para mitigar qual risco.
 - Negociar estratégias de mitigação, mesmo as que sejam menos eficazes, até que o custo faça sentido.

Exemplos de Risk Storming

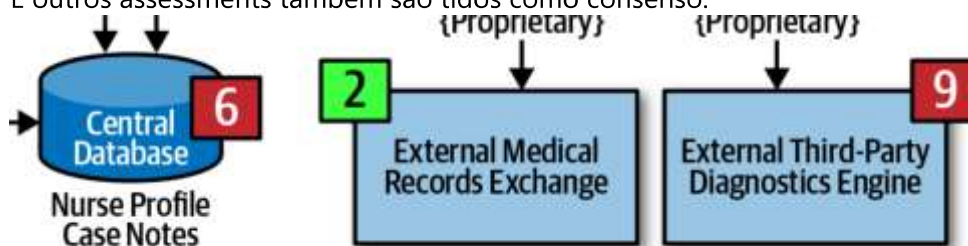
- Risk Storming não serve só pra arquitetura. Por exemplo jornada do usuário.
- Exemplo de arquitetura e estudo de caso:
 - Sistema de diagnósticos para enfermeiros.



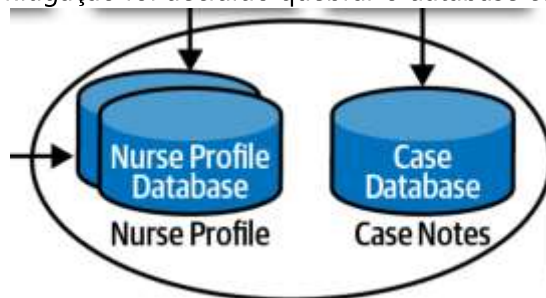
o *Figure 20-9. High-level architecture for nurse diagnostics system example*

Disponibilidade

- Database central foi identificado como risco nível 6
- E outros assessments também são tidos como consenso:



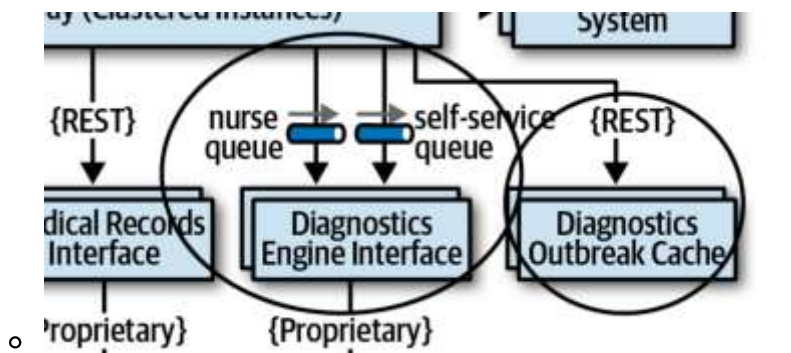
-
- Uma mitigação foi decidido quebrar o database central em dois databases diferentes.



- o
- Mas mitigar disponibilidade de recursos externos é bem mais complicado
 - o Após pesquisa concluiu-se que o risco é pequeno o suficiente para não ser mitigado.

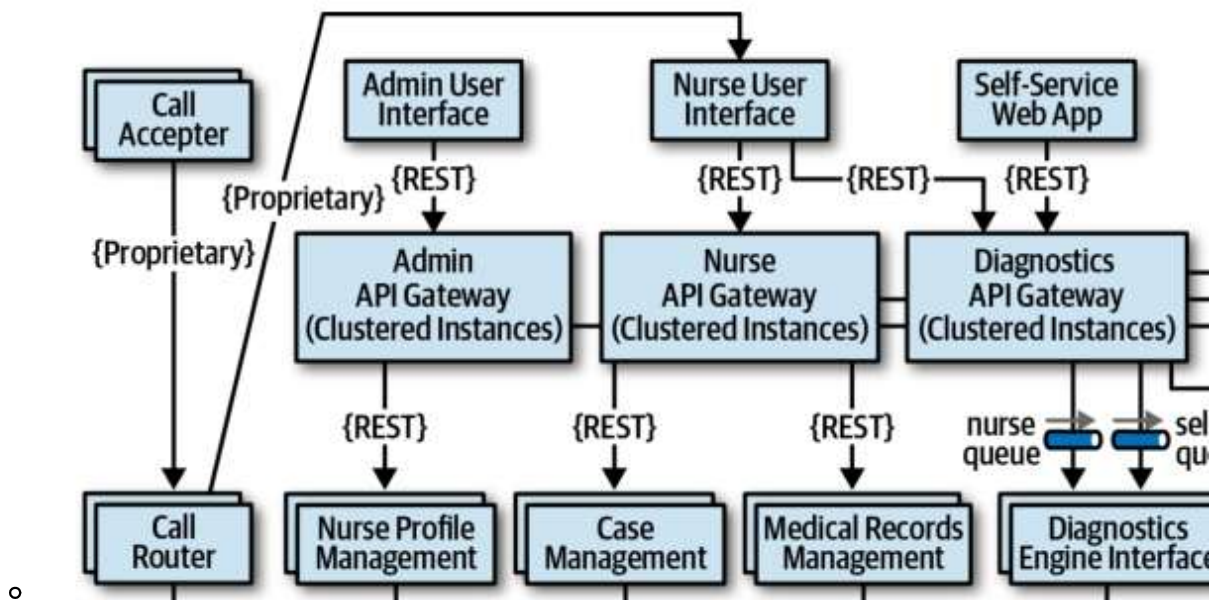
Elasticidade

- Problemas de surto de demanda (e.g. temporada de gripe)
- Identificou-se que interface não seria capaz de lidar com muitas requisições por segundo.
 - o Optou-se por criar sistema de filas



Segurança

- Regulação rígida de dados de saúde.
- Identificou-se API de diagnósticos como risco em potencial, contra a expectativa do arquiteto que considerava o sistema seguro.
 - Todos usuários usam a mesma API, podem acessar dados controlados.
- Para mitigar, separar API gateways por tipo de usuário para granularizar acesso e controle de segurança.



- Risk Storming é um processo contínuo ao longo do ciclo de vida de um sistema.