



A saga de quebrar aplicações em produção intencionalmente com Chaos Engineering

Alex Coqueiro

Head de Arquitetura de Soluções

AWS Setor Público – América Latina, Canadá e Caribe

 @alexbcbr



O que seu sistema deve fazer para não falhar?

Vamos testar para não fazê-lo falhar.

Revisitando um caso digital



IOError: Não há espaço no dispositivo

Fechar falhou no destructor de objeto de arquivo:

IOError: Não há espaço no dispositivo

Fechar falhou no destructor de objeto de arquivo:

IOError: Não há espaço no dispositivo

Fechar falhou no destructor de objeto de arquivo:

IOError: Não há espaço no dispositivo

Fechar falhou no destructor de objeto de arquivo:

IOError: Não há espaço no dispositivo

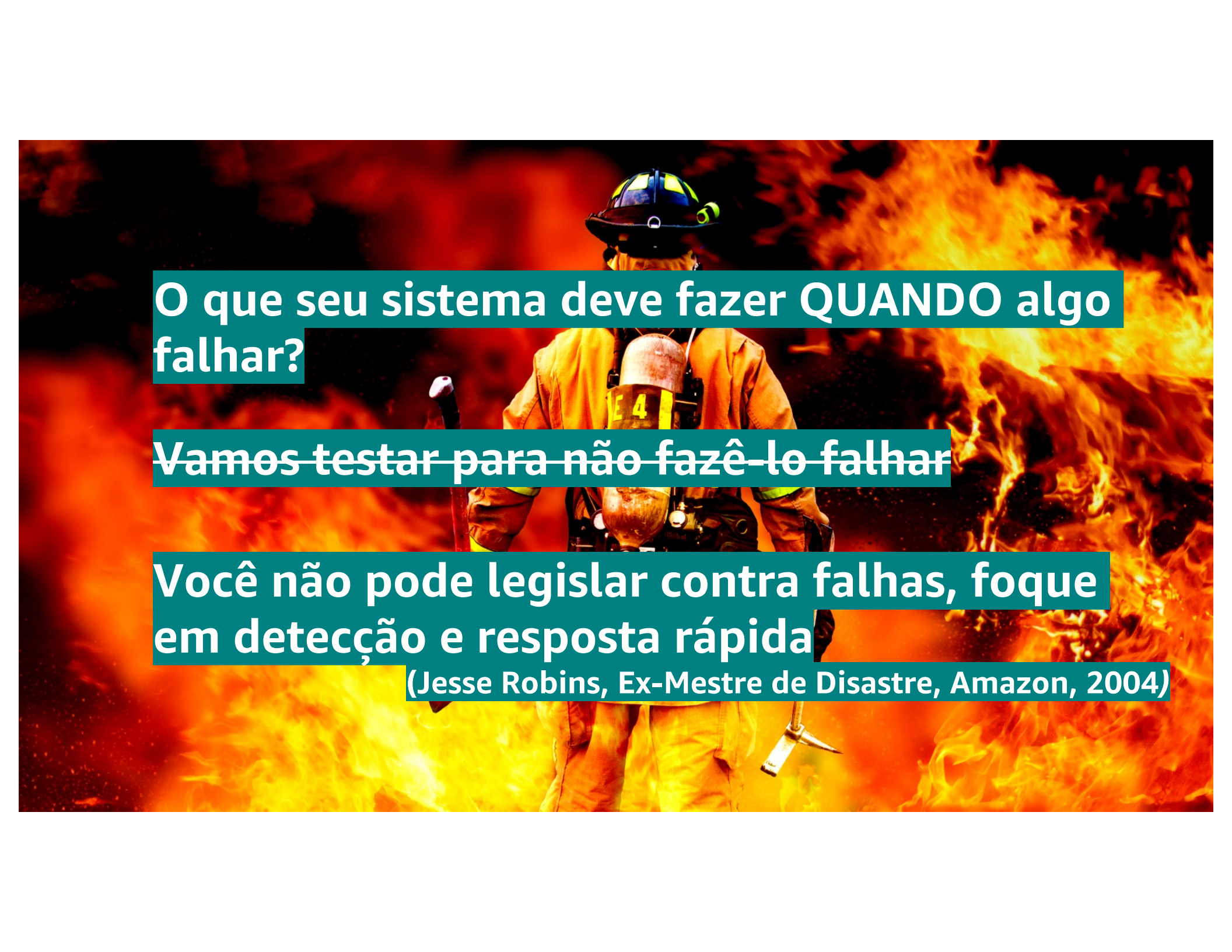
Fechar falhou no destructor de objeto de arquivo:

IOError: Não há espaço no dispositivo

Fechar falhou no destructor de objeto de arquivo:

IOError: Não há espaço no dispositivo

Fechar falhou no destructor de objeto de arquivo:



O que seu sistema deve fazer QUANDO algo falhar?

~~Vamos testar para não fazê-lo falhar~~

Você não pode legislar contra falhas, foque em detecção e resposta rápida

(Jesse Robins, Ex-Mestre de Desastre, Amazon, 2004)

A Era dos Macacos ...

"Exército Simian (Symian Army) criado para manter nossa nuvem segura e altamente disponível."

- 2011 Blog Netflix

Conjunto de agentes para:

- Derrubar serviços aleatoriamente
- Inserir latências
- Verificar a conformidade
- Quebrar uma região inteira (cloud)
- Integração com o pipeline de CI/CD (Spinnaker)



Chaos Engineering formalizada pela Netflix (2015)

PRINCIPLES OF CHAOS ENGINEERING

Last Update: 2018 May

Chaos Engineering is the discipline of experimenting on a system in order to build confidence in the system's capability to withstand turbulent conditions in production.

Advances in large-scale, distributed software systems are changing the game for software engineering. As an industry, we are quick to adopt practices that increase flexibility of development and velocity of deployment. An urgent question follows on the heels of these benefits: How much confidence we can have in the complex systems that we put into production?

Even when all of the individual services in a distributed system are functioning properly, the interactions between those services can cause unpredictable outcomes. Unpredictable outcomes, compounded by rare but disruptive real-world events that affect production environments, make these distributed systems inherently chaotic.

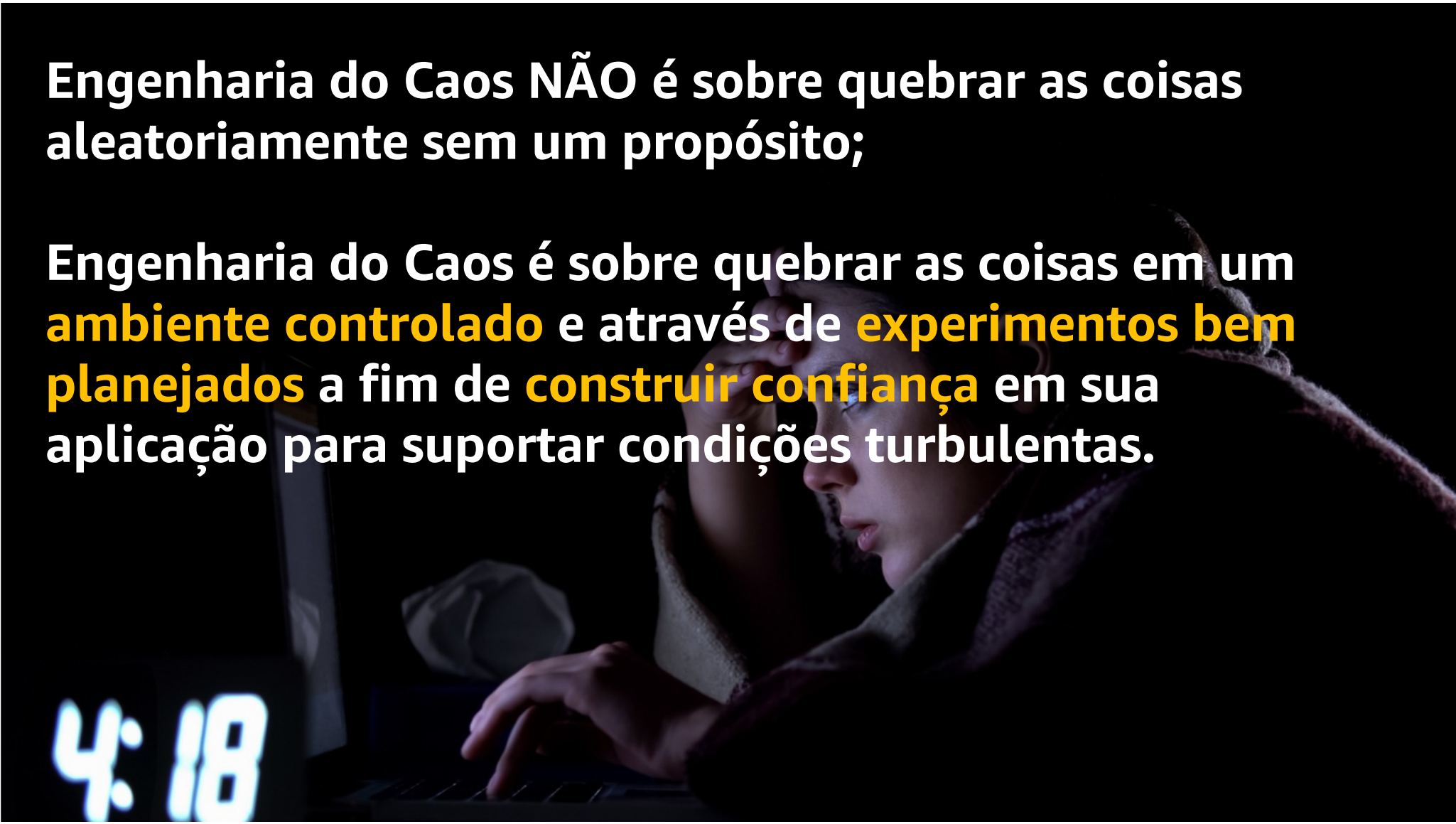
We need to identify weaknesses before they manifest in system-wide, aberrant behaviors. Systemic weaknesses could take the form of: improper fallback settings when a service is unavailable; retry storms from improperly tuned timeouts; outages when a downstream dependency receives too much traffic; cascading failures when a single point of failure crashes; etc. We must address the most significant weaknesses proactively, before they affect

principlesofchaos.org

Engenharia do Caos NÃO é sobre quebrar as coisas aleatoriamente sem um propósito;

Engenharia do Caos é sobre quebrar as coisas em um **ambiente controlado** e através de **experimentos bem planejados** a fim de **construir confiança** em sua aplicação para suportar condições turbulentas.

4:18

A person is shown in profile, working on a laptop in a dark environment. The person's hand is on the keyboard. In the bottom left corner, a digital clock displays '4:18' in bright blue numbers. The background is mostly black, with some faint light reflecting off the person's face and the laptop screen.

**“Chaos Engineering é a disciplina de
experimentação em sistemas distribuídos
a fim de construir confiança na capacidade
de suportar condições turbulentas na
produção.”**

<http://principlesofchaos.org>



Chaos Engineering



Melhorar a resiliência e o desempenho de aplicações



Descubra problemas desconhecidos



Preparar o time para situações críticas

Fases do Chaos Engineering



Fases do Chaos Engineering



Cenário de Caso de Uso – Eleições Governamentais

<http://eleicoes.abcgov.com.br>



Operação (Pessoas)

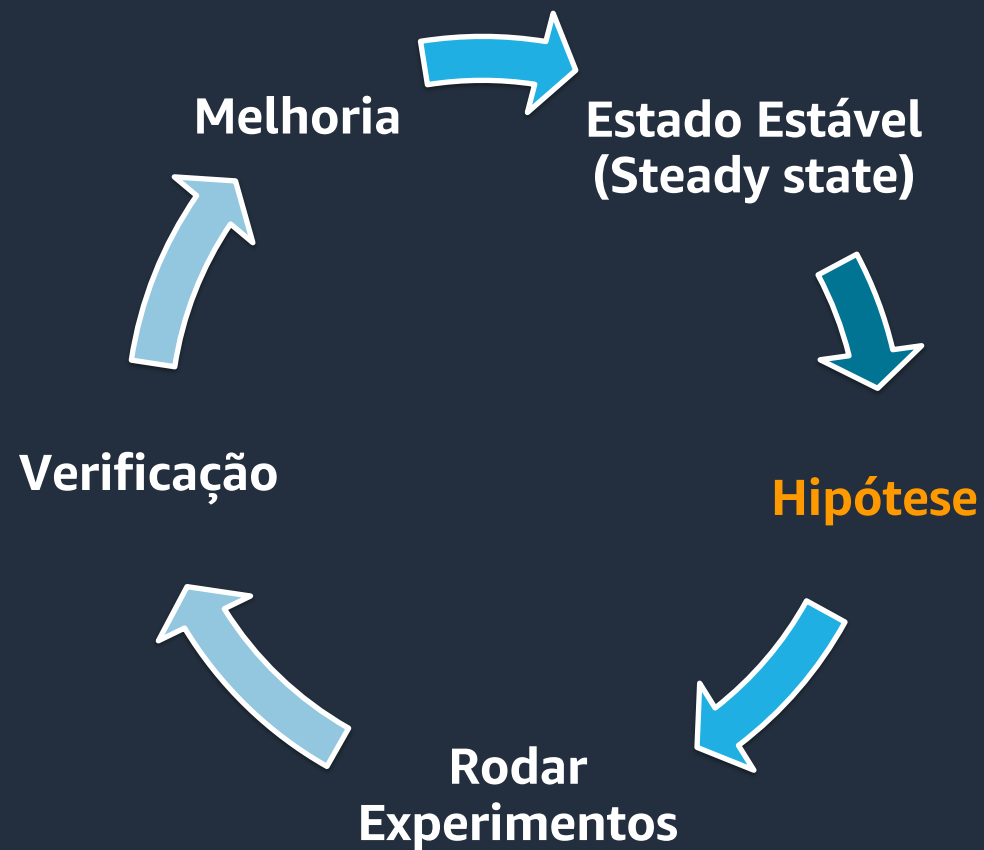
Aplicação

Switching

Infraestrutura



Fases do Chaos Engineering



Elaboramos hipóteses para lidar com incertezas ...

-

Shutting down

Infraestrutura

- Redundância
- Resiliência
- Isolamento
- Segurança

O voto será processado com sucesso (P99 <900ms) mesmo com 50% da capacidade indisponível

Switching

Porque?

Qualidade de Serviço (QoS)

Disjuntores (Circuit Breaker)

Porque a falha parcial não comprometeria a voto?

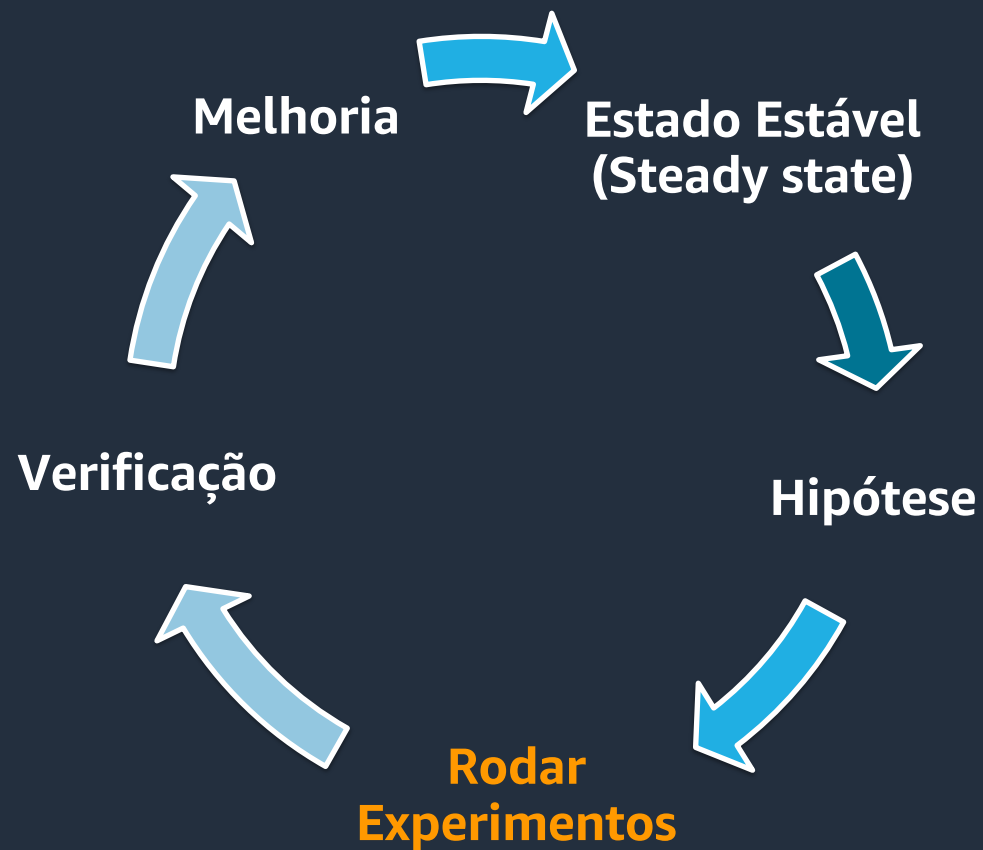
Aplicação

- Timeout
- Porque julgo que o processo de escalar vai funcionar?
- Stress de carga

Operação (Ops)

- Porque tenho confiança de que as métricas estão corretas?
- Monitoramento e observabilidade
- Resposta a incidentes
- Medir, medir, medir

Fases do Chaos Engineering



Como posso implementar a execução dos experimentos?

Operação (Pessoas)

Aplicação

Switching

Infraestrutura

Game Days

AWS Fault Injection Simulator

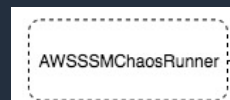


Chaos Mesh



Chaos Toolkit

Chaos Injection Layer for AWS Lambda - chaos_lib



Gremlin



ChaosBlade



Litmus

Security
Red Team



Infection Monkey
powered by Guardicore



SafeStack/ava



Cenário – Experimentando o impacto de falha no servidor



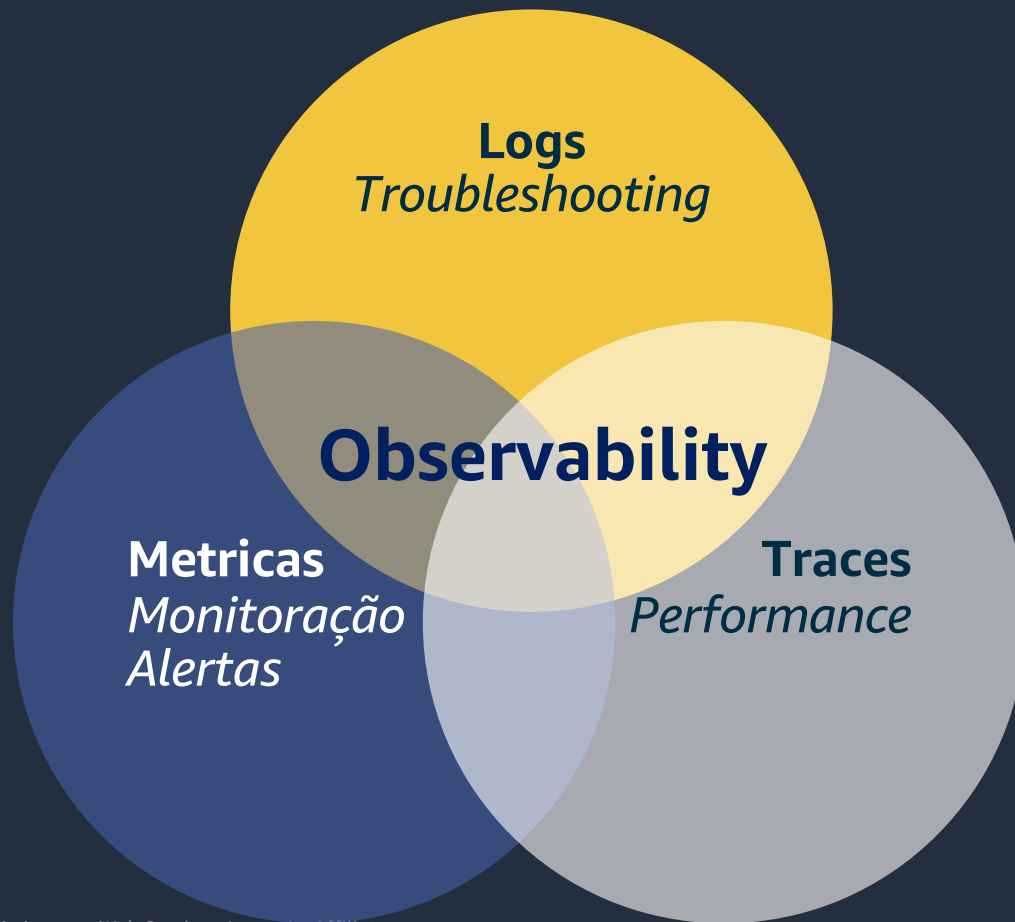
AWS



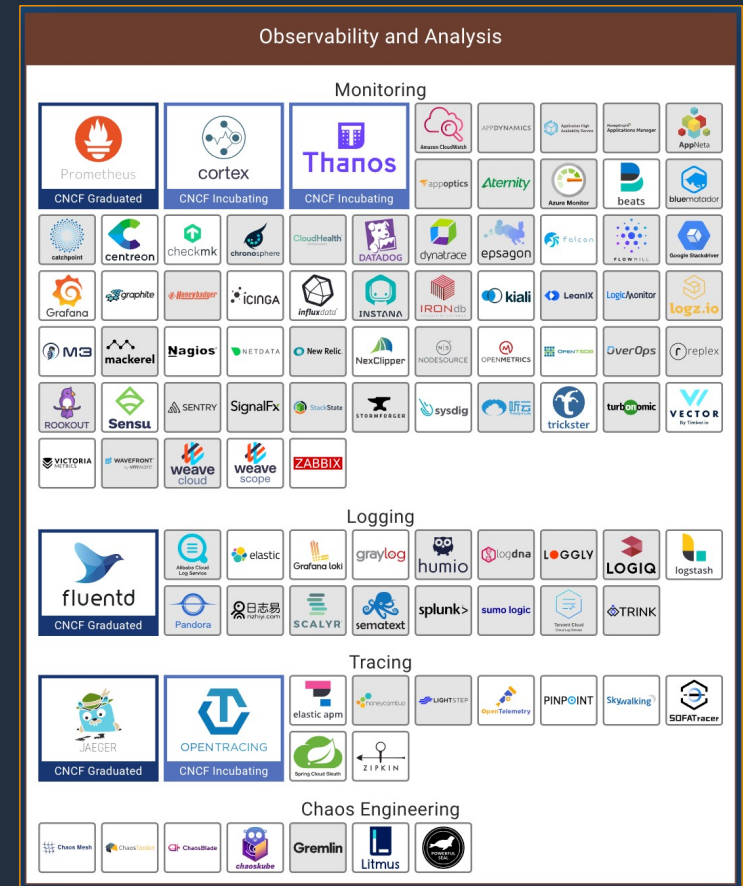
Fases do Chaos Engineering



Observability (Observabilidade)



© 2021, Amazon Web Services, Inc. or its Affiliates.



landscape.cncf.io



Cenário – Experimentando o impacto de falha no servidor



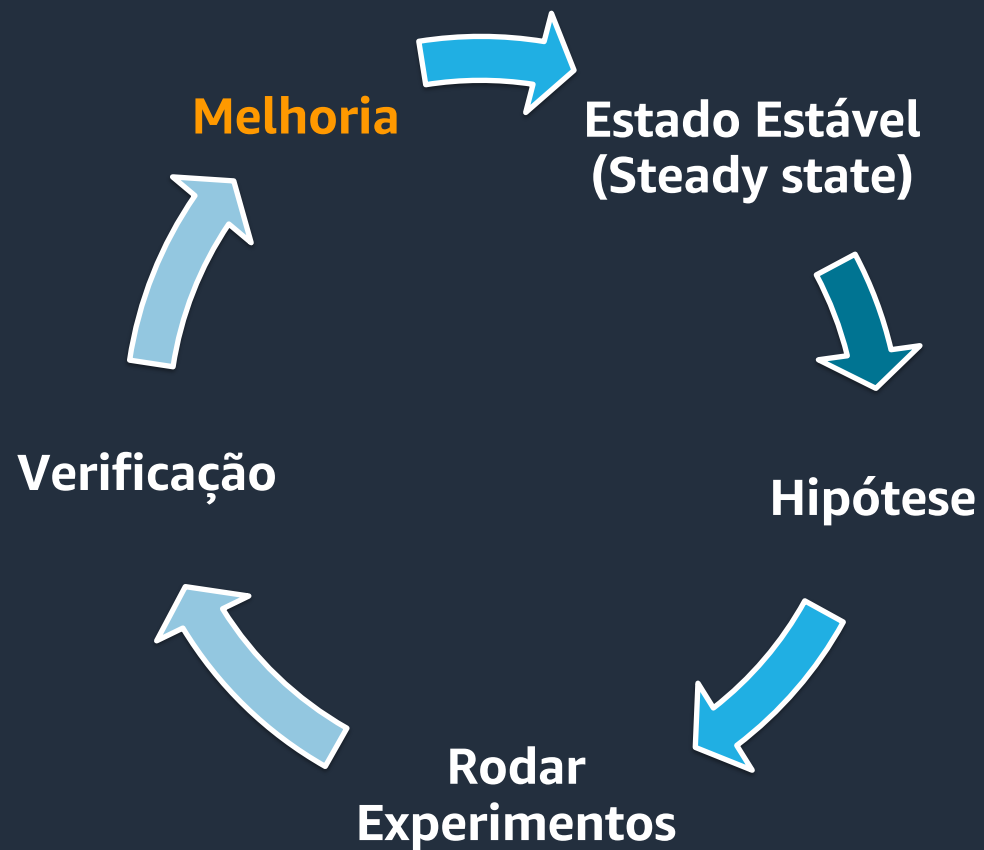
AWS



Outras coisas divertidas para fazer

- Bloqueia a resolução de DNS (`iptables -I OUTPUT -p udp -d <DNS server IP> --dport 53 -j GOTA`)
- Preencher o disco
- Corrupção de pacotes de rede (usando modelagem de tráfego)
- Matar processos aleatórios
- Desanexar (forçar) todos os volumes do EBS
- Bagunçar o `/etc/hosts`

Fases do Chaos Engineering



Dicas Importantes

- Comece com experimentos pequenos
- Procure estar o mais próximo possível da produção
- Minimize o Blast Radius
- Planeje a sua parada de emergência!
- Cuidado com estado que não pode ser revertido (dados corrompidos ou incorretos)



Fases do Chaos Engineering



A engenharia do caos é **NÃO** sobre quebrar coisas aleatoriamente **sem um propósito**, engenharia do caos é sobre quebrar as coisas em um **ambiente controlado** e através de **experimentos bem planejados** a fim de aumentar a confiança em sua aplicação para resistir a condições turbulentas.



Engenharia do Caos — Parte 1
Adrian Hornsby

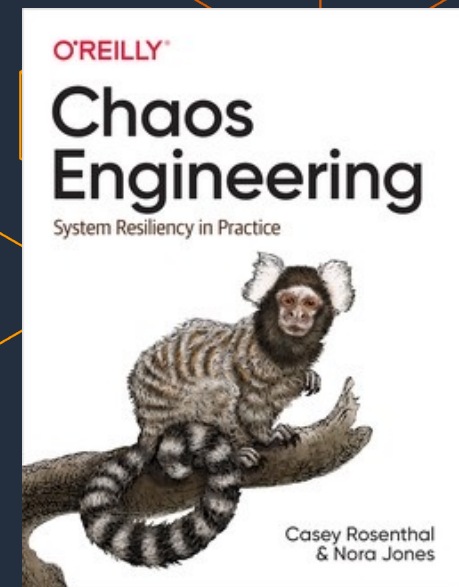
<https://medium.com.br/@adhorn/chaos-engenharia-ab0cc9fbd12a>

“O CAOS NÃO CAUSA PROBLEMAS. REVELA-OS.”

Nora Jones

Chaos Engineer and Senior Software Engineer at Netflix

© 2021, Amazon Web Services, Inc. or its Affiliates.





Muito Obrigado !!!

Alex Coqueiro

Head de Arquitetura de Soluções

AWS Setor Público – América Latina, Canadá e Caribe

 @alexbcbr