Avaliação da capacidade de sobrevivência a desastres em sistemas de *cloud computing* geograficamente distribuídos

Ana Carolina Veloso Teixeira acvt@cin.ufpe.br

Prof. Paulo Romero Martins Maciel prmm@cin.ufpe.br

UFPE

Centro de Informática

MoDCS

Agenda

- Motivação
- Objetivos
- Contextualização
- Modelos
- Próximos Passos

Motivação

- Atualmente, a demanda por recursos de nuvem está crescendo. Para prover a disponibilidade destes recursos, estudos vêm sendo feitos para melhorar os serviços prestados.

Motivação

- A importância de manter os dados ou serviços sempre à disposição dos clientes aumenta a cobrança sobre as empresas, para que esses serviços nunca parem de funcionar.
- A computação em nuvem trabalha com três tipos de modelos de negócio: IaaS, PaaS e SaaS.

Motivação

- Para garantir que esses serviços tenham seus níveis de qualidade atendidos, foi criado o SLA (Acordo de Nível de Serviço), que regula, por exemplo, o tempo máximo de inatividade. Provedores destes serviços devem levar também em consideração desastres, necessitando assim de um plano de recuperação de desastres (DRP).

Motivação

- Como avaliar a capacidade de sobrevivência de um *data center*, priorizando minimizar o tempo e o ponto de recuperação, para um plano desastre?

Objetivo

- Criar medologia/ferramenta que permita avaliação de *survivability* em ambientes de Iaas

Contextualização

- A recuperação de serviços de nuvem em um desastre é um problema persistente em plataformas de TI.
- Provedores de serviços em nuvem têm de fornecer os serviços a seus clientes mesmo que o *data center* não esteja funcionando devido a um desastre.

Contextualização

As empresas que fornecem serviços de Iaas estão lidando com possíveis desastres?

Contextualização

- Detectar quando um desastre ocorreu é um problema desafiador. Falhas transitórias ou segmentação de rede podem acionar alarmes falsos. Na prática, a maioria das técnicas de DR contam com mecanismos de detecção manual e *failover*.
- Nesta fase, o provedor de nuvem escolhe os mecanismos de recuperação, que impactam diretamente no RTO e RPO.

Contextualização

- Para as empresas o principal objetivo do *disaster recovery* é a continuidade dos serviços.
- Ou seja, retornar os serviços on-line depois de uma interrupção.
- O RTO*(Recovery Time Object)* e o RPO*(Recovery Point Object)* são dois importantes parâmetros que todo mecanismo de recuperação sempre tenta melhorar.

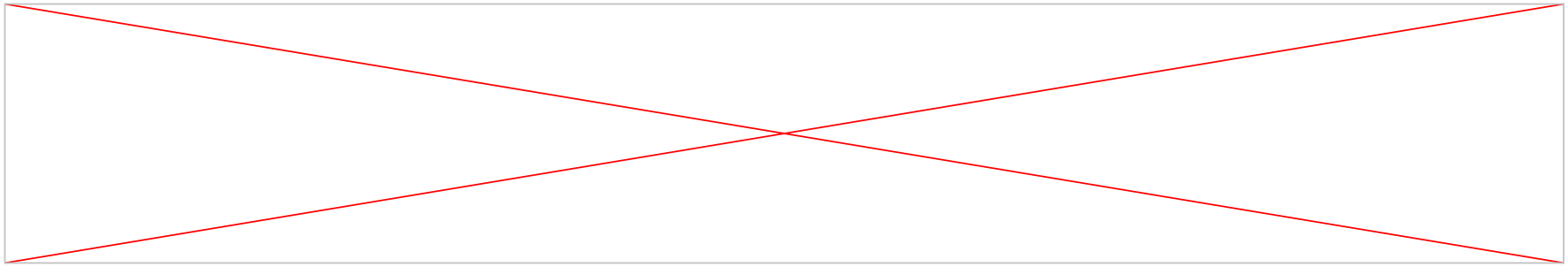
Contextualização

- Recovery Time Object (RTO) – Tempo que pode demorar para uma aplicação voltar a fornecer o serviço após a ocorrência de uma falha.
- Recovery Point Object (RPO) – Ponto no tempo da mais recente copia de segurança antes de qualquer falha.

Contextualização

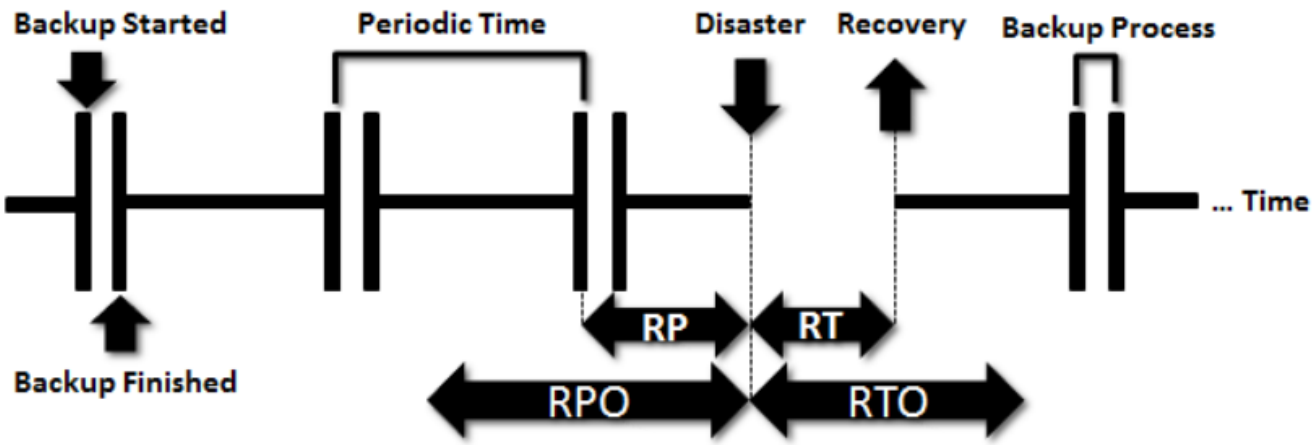
Recuperação de desastres de nível corporativo é medido principalmente em termos de Recovery Time Objective (RTO) e Recovery Point Objective (RPO).

Method/Pattern	RTO	Cost
Cold	Low RTO >= 1 business day	Lowest Cost
Pilot-Light	Moderate RTO < 4 hours	Moderate Cost
Warm	Aggressive RTO < 1 hour	Highest Cost



Contextualização

- *Recovery Point* $P_{RPO} = P\{R_p \leq RPO\} = P\{B_t \leq RPO - B_p\}.$
- *Recovery Time* $P_{RTO} = P\{R_t \leq RTO\}.$



Contextualização

- *Survivability*

  Capacidade que um sistema de computação tem de fornecer serviços essenciais na presença de ataques e / ou falhas, e recuperar o serviço por completo, em tempo hábil.

Métricas

- Não possui métrica fechada
- Combinação com outras métricas
- Trivedi mostra em um dos artigos passos para um procedimento geral para sobrevivência utilizando *Performability* e *Availability*

RTO e RPO?

Modelos

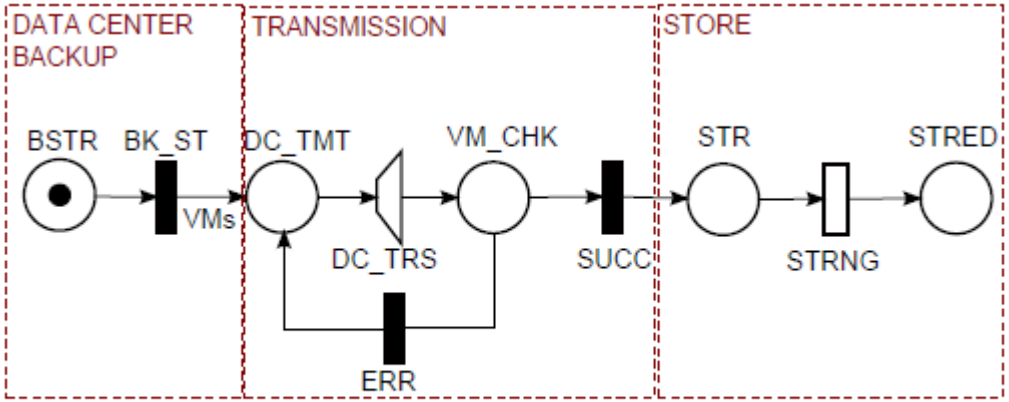


Figure 8: RPO Model

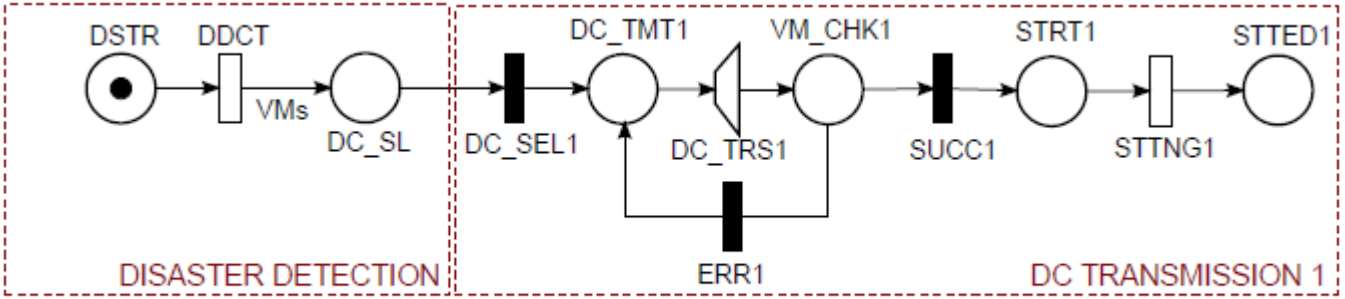


Figure 9: RTO Model

FIM