



CLOUD COMPUTING

Texto base

8

Backup e Recuperação

Prof. Me. Rodolfo Riyoei Goya

Resumo

Na Tecnologia da Informação (T.I.), uma das atividades mais importantes é a produção de cópias de segurança (Backups), para a recuperação de situações de desastre ou perda catastrófica. A “Computação em Nuvem” proporciona maneiras econômicas, práticas e seguras para executá-la. Abordam-se aqui, como o backup e a recuperação de desastre pode ser realizado na nuvem, através de serviços da AWS.

8.1. Introdução

Quando se trata de segurança de T.I., atividades para proteção contra perda catastrófica de dados são essenciais. Como serviços de “Computação em Nuvem”, como armazenamento, controle de ciclo de vida, proteção por criptografia e ferramentas para gerenciar imagens podem ser úteis para tal proteção? Como proteger imagens de máquinas virtuais em execução na “Nuvem”? Quais estratégias existem?

Com a proliferação dos serviços de nuvens, a cultura de usar imagens como blocos padrão para movimentação de dados e a disponibilidade de serviços baratos de armazenamento se tornaram muito comuns. Com isso, ambos passaram a fazer parte dos cenários para procedimentos de backup e recuperação de desastres. Na arquitetura da AWS, as estratégias para backup e recuperação usando nuvens apresentadas são quatro (em ordem crescente de custos e decrescente de tempo de recuperação):

- a. Backup and Restore
- b. Pilot light
- c. Warm standby
- d. Multi site

8.2. Backup and Restore

No cenário “Backup and Restore”, os dados a serem protegidos estão em infraestrutura on premises. A boa prática exige que os backups sejam armazenados em outro local, neste caso, na nuvem. Em caso de desastre, este cenário apresenta um período em que os serviços estão indisponíveis: o tempo necessário para recuperar a infraestrutura e trazer de volta os dados da nuvem. Para suporte a esse cenário, a AWS dispõe dos serviços Storage Gateway e Glacier.

8.2.1. AWS Storage Gateway

O Storage Gateway é um serviço que implementa um armazenamento virtual para uma infraestrutura “on premises”. Pode ser disponibilizado na forma de um programa de aplicação instalado em um servidor local ou como um “appliance” (uma caixa ligada na rede local contendo tudo o que é preciso dentro dela).

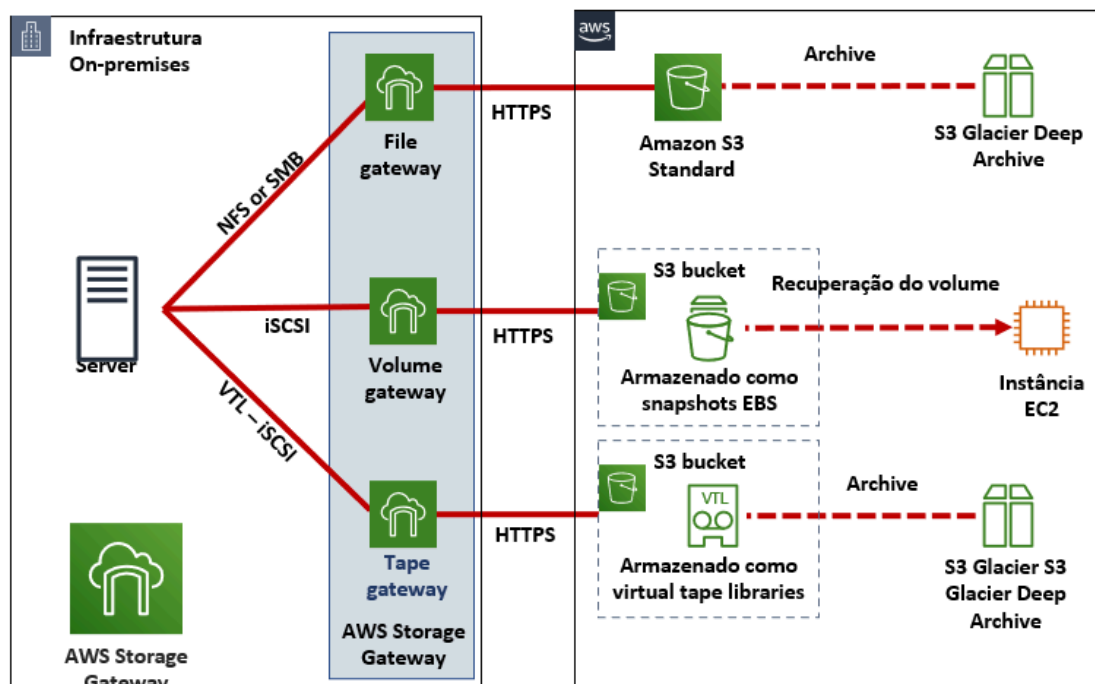
O Storage Gateway se comunica com a nuvem através de conexão criptografada (por HTTPS sobre SSL) onde fica o armazenamento físico. Com isso, o armazenamento virtual dá a impressão dos dados estarem disponíveis como se estivessem em armazenamento local.

O Storage Gateway virtualiza o armazenamento remoto de três modos diferentes:

- a. File gateway: Volume de S.O. virtual via SMB (Windows) ou NFS (Linux)
- b. Volume gateway: Volume de HD virtual (SCSI)
- c. Tape gateway: Unidade de Fita virtual (VTL)

Destes modos, um servidor local troca dados com o Storage Gateway do mesmo modo como o faria com uma unidade de fita ou HD externo ou montaria um volume NFS em outro servidor local. Os casos de uso do Storage Gateway estão descritos na Figura 1.

Figura 1. Tela Inicial do Console da AWS



Fonte: do autor, 2022.

8.2.2. S3 Glacier

Para armazenamento de alta durabilidade e baixíssimo custo para dados com acesso pouco frequente, o S3 Glacier é o serviço da AWS mais adequado. Além de oferecer os mesmos serviços do S3 (como controle de versão e criptografia), é um produto de escalabilidade ilimitada, armazenamento distribuído replicado em múltiplas regiões e com durabilidade de 99.999999999% (11 9's). É disponibilizado em três categorias:

- S3 Glacier Instant Retrieval: recuperação de dados em milissegundos.
- S3 Glacier Flexible Retrieval: recuperação de dados em minutos (em versão gratuita, de 5 e 12 horas).
- S3 Glacier Deep Archive: recuperação de dados em até 12 horas.

8.3. Pilot Lamp

No cenário de backup e recuperação “Pilot Lamp”, os dados a serem protegidos podem estar on premisses ou em nuvem com recuperação feita usando serviços em nuvem. Neste cenário, é feita cópia de imagens das máquinas virtuais em operação e backup dos dados, tudo mantido no site de recuperação. As máquinas virtuais são criadas na nuvem na hora da situação de desastre (se a operação regular for em nuvem, a recuperação deverá se dar em outra zona de disponibilidade ou região), o que pode aumentar o tempo requerido para a recuperação: em caso de desastre, este cenário apresenta um período enquanto as novas máquinas virtuais são criadas e suas imagens carregadas, em que os serviços estão indisponíveis.

8.3.1. Preparação

Para este cenário, a preparação consiste em:

- a. Documentar e atualizar continuamente as imagens dos servidores para pronta recuperação em caso de desastre.
- b. Manter réplica atualizada dos bancos de dados.
- c. Planejar recuperação, incluindo reconfiguração de DNS, se necessário.
- d. Considerar o uso de scripts e procedimentos automatizados para acelerar a recuperação.

8.3.2. Recuperação de desastre

Para este cenário, a recuperação consiste em:

- a. Instalar servidores em máquinas virtuais e recuperar as imagens.
- b. Escalar o sistema para atender o porte da operação.
- c. Ativar réplica dos bancos de dados.
- d. Reconfiguração de DNS, se necessário.

8.4. Warm Standby

No cenário de backup e recuperação “Warm Standby”, como no “Pilot Lamp”, os dados protegidos podem estar on premisses ou em nuvem e o cenário de recuperação é em nuvem. A diferença é que uma pequena capacidade dos servidores de recuperação é mantida em operação.

Em caso de desastre, os serviços são redirecionados para o site de recuperação (por exemplo, via reconfiguração de DNS) após o qual um redimensionamento pode ser exigido. Este cenário apresenta um pequeno período em que os serviços estão indisponíveis durante a detecção da queda e mudança para o site de recuperação.

8.4.1. Preparação

Para este cenário, a preparação consiste em:

- a. Atualizar continuamente as imagens dos servidores no site de recuperação.
- b. Manter réplica atualizada dos bancos de dados.
- c. Considerar o uso de scripts, testes e procedimentos automatizados para acelerar a recuperação.

8.4.2. Recuperação de desastre

Para este cenário, a recuperação consiste em:

- a. Reconfiguração de DNS, se necessário.
- b. Escalar o sistema para atender o porte da operação.

8.5. Multi-site

No cenário “Multi-site”, há múltiplos sites (“N+1”) em diferentes regiões ou zonas de disponibilidade operando com balanço de carga e o cenário de recuperação consiste nos demais “N” sites darem conta da perda de algum dos sites. Todos os servidores são mantidos em operação. Mesmo em caso de desastre, os serviços estão sempre disponíveis. Este cenário é o de menor tempo de recuperação, mas é o mais complexo de se manter e de maior custo de operação.

8.5.1. Preparação

Para este cenário, a preparação consiste em:

- Atualizar continuamente as imagens dos servidores em todos os sites.
- Manter réplica atualizada dos bancos de dados.
- Considerar o uso de scripts, testes e procedimentos automatizados para acelerar a recuperação.

8.5.2. Recuperação de desastre

Para este cenário, a recuperação consiste em:

- Reconfiguração de DNS, se necessário.
- Escalar o sistema para atender o porte da operação.

8.6. Vamos praticar?

8.6.1. Quanto custa fazer backup no serviço AWS Glacier?

Vá ao site da AWS e veja qual é o custo mensal dos serviços de armazenamento no S3 Glacier. Experimente, digamos, ver o custo para 500 GBytes por mês. Note que o custo pode variar para diferentes regiões.

<https://aws.amazon.com/pt/s3/pricing/>

8.6.2. Faça uma imagem de um volume EBS

Volumes em EBS podem ser usados em EC2. Para fazer o backup de um volume, o método mais direto é produzir uma imagem (“snapshot”) e guardá-la em um bucket S3. Veja mais detalhes no link:

<https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ec2-ug.pdf#EBSSnapshots>

8.7. Você quer ler?

8.7.1. Quer saber mais sobre backup na nuvem?

Quem tem toda a instalação “On Premises” (sem usar serviços em nuvem), também pode usar backup em nuvem em arranjos híbridos com unidades de fita virtualizadas. Quer saber mais? Veja mais detalhes no link:

<https://aws.amazon.com/pt/storagegateway/vtl/>

8.7.2. Que é gerenciamento de ciclo de vida?

Dados armazenados na nuvem podem ter um controle mais preciso do que é guardado em backup e o que ficou obsoleto e pode ser descartado. Além disso, dados podem ser movidos para diferentes tipos de armazenamento de acordo com seus requisitos de disponibilidade ou custo. Tudo isso é feito pelos serviços de valor agregado do S3. Veja mais detalhes nos links:

https://aws.amazon.com/pt/s3/features/#Storage_Management

Referências

- TAURION, Cezar. **Cloud Computing**: computação em nuvem: transformando o mundo da tecnologia da informação. Rio de Janeiro: Brasport, 2009.
- VELTE, Anthony T.; VELTE, Toby J.; ELSENPETER, Robert. **Cloud Computing**: a practical approach. EUA:McGraw-Hill, 2010.
- MARSHALL, Nick; BROWN, Mike; BLAIR FRITZ, G.; JOHNSON, Ryan. **Mastering VMware vSphere 6.7**. New Jersey: Sybex, 2019. 848p.
- SANTOS, Tiago. **Fundamentos da computação em nuvem** (Série Universitária). São Paulo, Editora Senac, 2018. 211p.
- ANDREWS, Joshua; HALL, Jon. **VMware Certified Professional Data Center Virtualization on vSphere 6.7 Study Guide**: Exam 2V0-21.19. 1.ed. New Jersey: Sybex, 2020. 640p.
- Official Amazon Web Services (AWS) Documentation. **Simple Storage Service User Guide**. Amazon. 1.502p. Disponível em: <https://docs.aws.amazon.com/AmazonS3/latest/userguide/s3-userguide.pdf> acessado em 17/03/2022.
- Official Amazon Web Services (AWS) Documentation. **AWS Storage Gateway User Guide**. Amazon. 427p. Disponível em: <https://docs.aws.amazon.com/storagegateway/latest/userguide/storagegateway-ug.pdf> acessado em 17/03/2022.