

PLANO DE CONTINGÊNCIA BIBLIOTECA VIRTUAL UNIVERSITÁRIA - PEARSON

1. Disaster Recovery and Contingency Plan – Biblioteca Virtual v.4

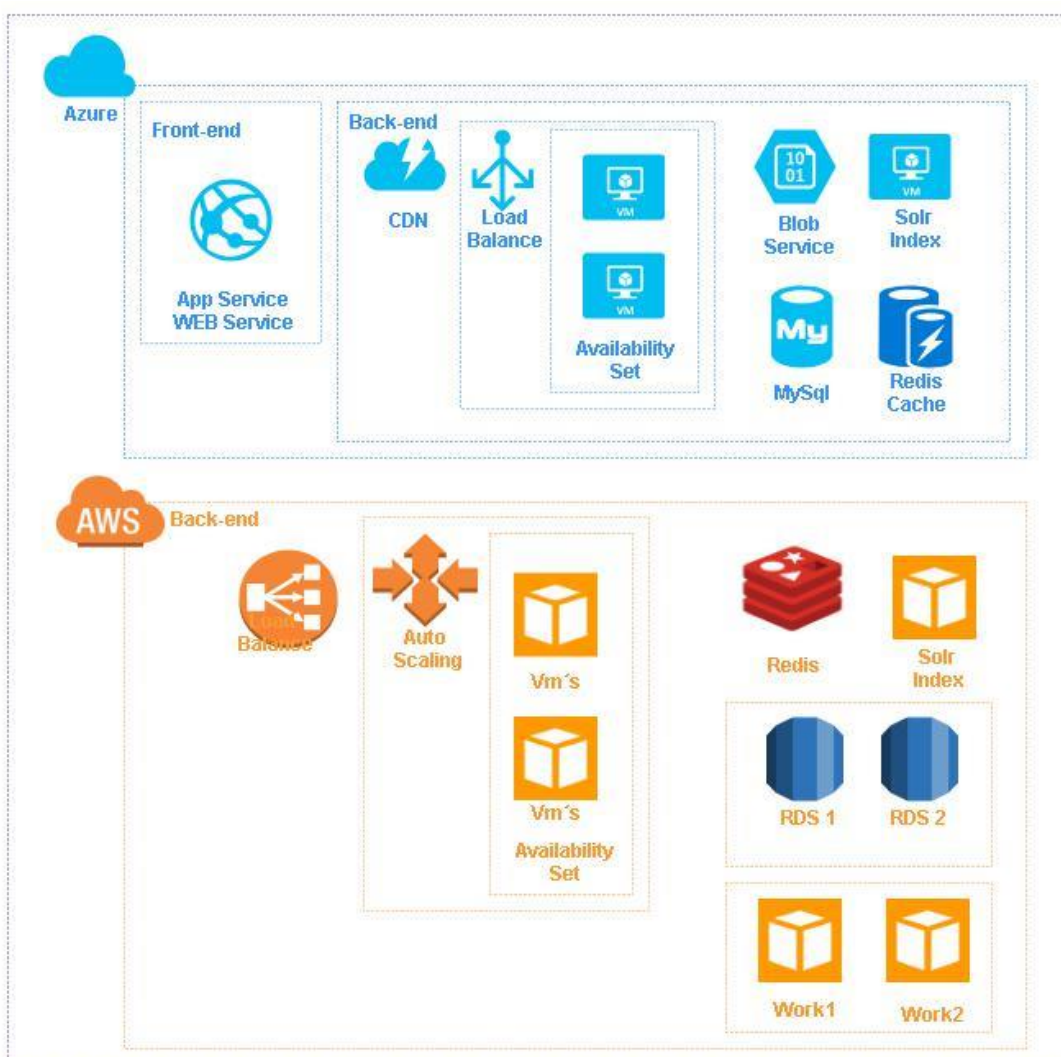
1. Arquitetura Disaster Recovery Biblioteca Virtual v.4.

Atualmente a plataforma BV4 utiliza os serviços das nuvens Azure e AWS. Esses serviços garantem escalabilidade, redundância e disponibilidade dos recursos em 98% do tempo.

Glossário:

- Escalabilidade. Em engenharia de software, escalabilidade é uma característica desejável em todo o sistema, em uma rede ou em um processo, que indica sua habilidade de manipular uma porção crescente de trabalho de forma uniforme, ou estar preparado para crescer conforme a demanda;
- Disponibilidade, é a característica onde, por um acordo de nível de serviço um sistema ou plataforma fica acessível aos seus clientes finais, esse tempo é pode ser medido em horas ao logo de um período;
- Redundância, tem por objetivo garantir a funcionalidade e operacionalidade do sistema em caso de uma falha em um ou mais partes que envolvem o sistema ou plataforma;

Arquitetura em nuvem Azure e AWS



Recursos utilizados:

- Azure
 - App Services
 - CDN, Load Balance
 - MySql Service Redis Cache
 - Blob Service
- AWS
 - Load Balance
 - Auto Scaling RDS

2. A política de backup visa a garantir a recuperação dos dados e a restauração do ambiente no menor tempo possível, caso alguma falha grave na arquitetura ocorra. Como política de backup, a Digital Pages utiliza os melhores softwares, mecanismos e estratégias, conforme descrito abaixo:

2.1. Banco de dados.

Para a realização do backup dos dados, é utilizada a ferramenta Jenkins. A periodicidade e a política de retenção dos arquivos de backup se dão conforme a tabela abaixo. Além do backup realizado pela Digital Pages, a Azure também possui seu próprio esquema de backup.

Tipo	Descritivo	Periodicidade	Retenção
Digital Pages (Completo)	Os backups de banco de dados completos ocorrem em:	Diário	3 meses
		Semanal	3 meses
		Mensal	1 ano
		Bimestral	1 ano
		Trimestral	1 ano
		Semestral	5 anos
		Anual	5 anos
Azure / AWS (Completo)	Os backups de banco de dados completos ocorrem semanalmente	Semanal	35 dias
Azure / AWS (Diferencial)	os backups de banco de dados diferenciais geralmente ocorrem em horários determinados		35 dias
Logs	os backups de log de transações geralmente ocorrem a cada 5 a 10 minutos	5 - 10 minutos	35 dias

2.2. Disaster recovery

Toda a infraestrutura foi mapeada por meio de scripts de automação, que permitem recuperar o ambiente rapidamente, em caso de um incidente, da necessidade de recuperação de um serviço, componente ou provisionamento de novos serviços.

Script	componente	Periodicidade
RDP Infrastructure	Resource Group	a cada mudança
	Network security group	
	Virtual network	

Virtual network

Conta de armazenamento (Blob)

Máquinas Virtuais

Load Balance

Application Deploy

RDP Infrastructure DB	Cache Redis	a cada mudança
	CDN	
	Deploy aplicações	
	MySQL como serviço	
	Import Database	

2.3. Local de armazenamento dos backups.

Todos os arquivos de backup são armazenados na nuvem Azure em pastas do Blob, seguindo uma nomenclatura única para cada arquivo.

Conforme a política de retenção, os arquivos são eliminados das pastas.

Pasta de backup	Nome do arquivo	Retenção
RDP-BKP_Diario	RDP-BKP_diario_dd-mm-yyyy	3 meses
RDP-BKP_Semanal	RDP-BKP_semanal_dd-mm-yyyy	3 meses
RDP-BKP_Mensal	RDP-BKP_mensal_dd-mm-yyyy	1 ano
RDP-BKP_Bimestral	RDP-BKP_bimestral_dd-mm-yyyy	1 ano
RDP-BKP_Trimestral	RDP-BKP_trimestral_dd-mm-yyyy	1 ano
RDP-BKP_Semenstral	RDP-BKP_semenstral_dd-mm-yyyy	5 anos
RDP-BKP_Anual	RDP-BKP_anual_dd-mm-yyyy	5 anos

3.0 Principais Recursos para inibição de desastre

- Todos os serviços e processos rodam em nuvem pela AWS e Azure;
- Os sistemas contam com redundância, incluindo redundância geográfica;
- DNS Failover para garantir a entrega imediata dos recursos de redundância;
- Treinamento e capacitação da equipe em Segurança da Informação
- Revisão de toda infraestrutura, códigos e serviços envolvidos.
- Aplicação de patches de segurança e prevenção nos servidores e equipamentos
- Monitoramento 24/7 de todos os serviços e processos
- Infraestrutura dinamicamente alocada de acordo com a montante de acessos na plataforma.