UserStory 810. – Realizado por António Sousa – 1060694

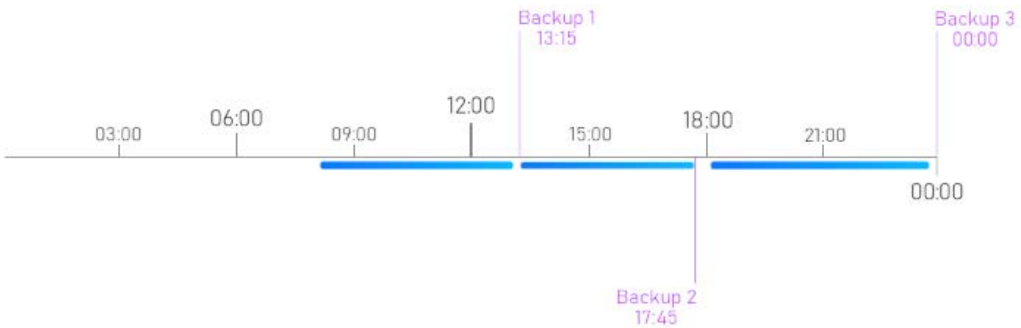
"Como administrador do sistema quero que seja proposta, justificada e implementada uma estratégia de cópia de segurança que minimize o RPO (Recovery Point Objective) e o WRT (Work Recovery Time)"

R: Para o sistema em questão, e mediante as cargas horárias das atividades letivas estabelecidas pelos vários departamentos do campus, pressupõe-se que o sistema poderá ser utilizado entre as 08:00 e as 23:30, com uma breve interrupção entre as 13:00 e as 13:30 para a transição das turmas da manhã para a tarde, e outra interrupção entre as 17:30 e as 18:00 para transição para as turmas da noite. Com base nesta premissa, será proposta a seguinte estratégia:

Frequência dos backups: Por forma a minimizar o tempo máximo de perda de dados, irá realizar-se o backup de todo o sistema três vezes por dia. O primeiro será programado para as 13:15, período em que é espectável pouca ou praticamente nenhuma utilização da plataforma. O segundo será agendado para as 17:45, período análogo ao anterior, e o terceiro será agendado para as 00:00 horas, período em que não se espera de forma alguma utilização da plataforma visto todos os serviços do campus se encontrarem encerrados.

Tendo em conta esta configuração, é possível obtermos um **RPO** máximo de sensivelmente 5 horas para qualquer um dos períodos de maior atividade, sem que seja notório o período de indisponibilidade do sistema para efeitos de backup, tornando a experiência de utilização da plataforma praticamente fluída e ininterrupta, e ao mesmo tempo segura.

Figura 1- Vista do agendamento dos backups diários tendo em conta períodos de atividade letiva



Natureza dos backups: Uma vez que, toda a aplicação inclusive o export da base de dados, ocupa sensivelmente um espaço físico em disco inferior a 500MBs, todos os backups sem exceção podem ser completos (Full). Num servidor de capacidade mediana, um backup desta natureza leva não mais do que alguns minutos (< 5 minutos) e como tal, realizando apenas backups desta natureza, também o seu restauro será igualmente mais rápido no caso de ser necessário a sua reposição, uma vez que se trata de um único ficheiro e não ser necessário restaurar juntamente com backups incrementais. Desta forma o **WRT** será semelhante ao tempo da realização do backup, e poderá levar na melhor das hipóteses alguns minutos (também inferior a 5). No caso

"Como administrador do sistema quero que seja proposta, justificada e implementada uma estratégia de cópia de segurança que minimize o RPO (Recovery Point Objective) e o WRT (Work Recovery Time)"

de se estar a recuperar de um desastre, em que o próprio servidor ficou inutilizado, deverão ter-se em contra outros fatores como:

- Instalação e configuração do sistema operativo num outro servidor (30 – 60 minutos)
- Instalação e configuração de um servidor Web Apache / Nginx (10 – 20 minutos)
- Instalação da base de dados mongoDB (5 – 10 minutos)
- Restauro da base de dados do backup (1 – 5 minutos)
- Restauro e configuração da aplicação (5 – 10 minutos)
- Testes sobre o restauro da aplicação e dados (5 – 10 minutos)

Portanto, estima-se que possa haver, em situações ideais, um downtime entre uma e duas horas para o **WRT** em caso de recuperação de desastre.

Armazenamento e segurança dos backups: Por forma a garantir redundância dos backups, cada backup será replicado para um repositório offsite (fora das instalações onde a plataforma se encontra). O processo será feito via *scp*, programado por via de um *script* e agendado em *crontab.*

Script de backup: Para a concretização do backup, o seguinte script (Bash) será invocado:

```
#!/bin/bash

# nome do ficheiro de backup (incluirá data e hora)
filename="robdronego_$(date +%d%m%y_%H%I).tar.gz"

# pasta da aplicação
appfolder="/home/code/nodejs"

# pasta de backup
bkupfolder="/home/bkup"

# ip do servidor remoto para backup
remoteip=10.1.2.3

# pasta no servidor remoto para backup
remotefolder="/home/bkup"

# execução do backup
tar -zcvf "$bkupfolder/$filename" $appfolder

# cópia offsite do backup (pressupõe-se que o ssh está previamente
# configurado para evitar solicitação de password durante a cópia)
scp $bkupfolder/$filename root@$remoteip:$remotefolder
```

UserStory 810. – Realizado por António Sousa – 1060694

"Como administrador do sistema quero que seja proposta, justificada e implementada uma estratégia de cópia de segurança que minimize o RPO (Recovery Point Objective) e o WRT (Work Recovery Time)"

Agendamento do backup (via Crontab):

```
# For more information see the manual pages of crontab(5) and cron(8)
#
# m h  dom mon dow   command

15 13 * * * /usr/local/sbin/robdronego.sh
45 17 * * * /usr/local/sbin/robdronego.sh
00 00 * * * /usr/local/sbin/robdronego.sh

~
```

Propostas de melhoramento do serviço de backups:

- No sentido de melhorar o serviço de backup, é possível implementar também um sistema de registo (Logs) da ocorrência do backup. Desta forma, podemos monitorizar se ocorreu uma falha em qualquer parte do script de execução do backup.
- É ainda possível encriptar o ficheiro resultante por forma a impedir o acesso não autorizado aos dados da aplicação constantes no backup.